EXHIBIT A

Arizona Senate Audit

Digital Findings

Presented By Ben Cotton

Arizona Senate Audit

- Withheld Devices and Data
- Cyber Security Issues
- Hardware Configuration Control
- File Deletions
- Failure to Preserve Election Artifacts
- Anonymous Logins
- Listening Ports and Attempted Connections on Bootup
- Internet Connections and History

Withheld Devices and Data

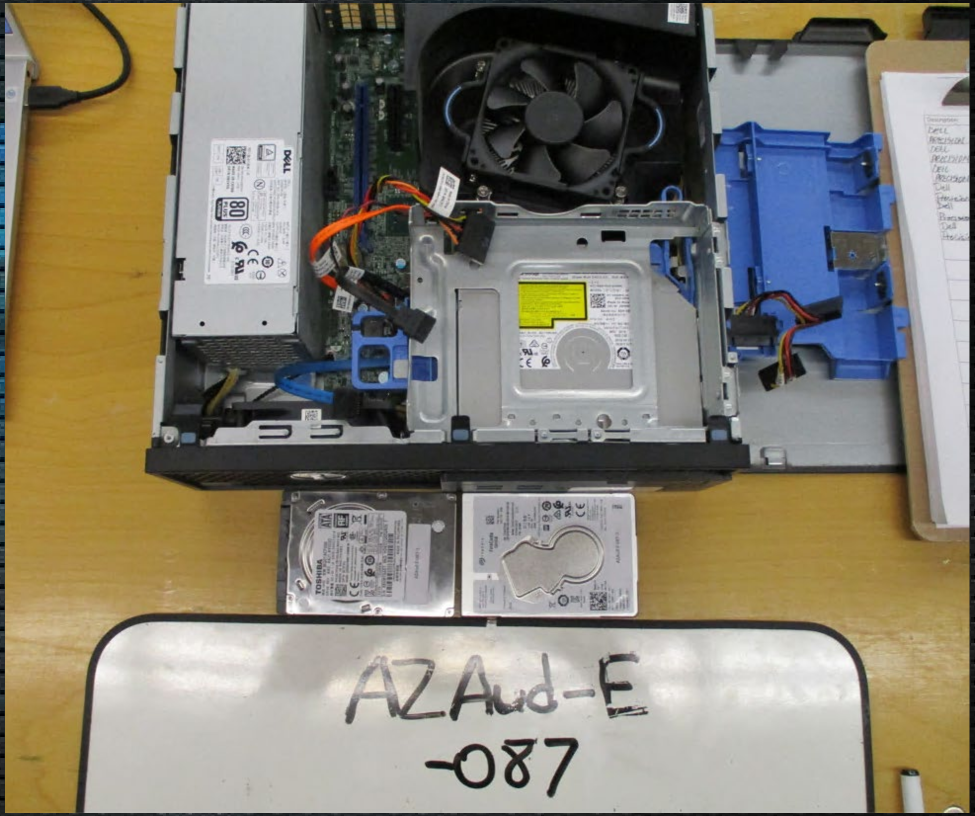
- Routers and Network Related Data
- Poll Worker Laptops
- ICX Devices
- ICP Credentials to Validate Configuration Settings or Administrative Settings
- Other Devices Connected to Election Network
  - 192.168.100.1
  - 192.168.100.11

Cyber Security Issues

- Failed to Perform Basic OS Patch Management
- Failed to Update AntiVirus Definitions
- EAC Certification Defense is NOT Valid In View of the Evidence
  - 4 .exe Files Created After Dominion Software Install
  - 45 .exe Files Modified After Dominion Software Install
  - 377 .dll Files Created After Dominion Software Install
  - 1053 .dll Files Modified After Dominion Software Install
- Log Management - Failed to Preserve Security Logs
- Credential Management – Shared Accounts and Common Passwords
- Failed to Establish and Monitor Host Baseline
- Failed to Establish and Monitor Network Communications Baseline

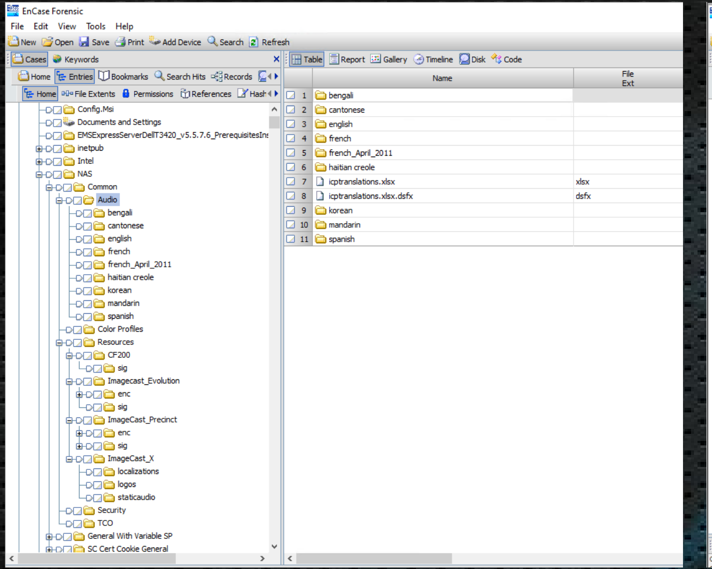
Hardware Configuration Issues

- Dual Boot Configuration Discovered on Adjudication 02 Endpoint
  - Two Hard Drives Internal to System
  - Both Drives Bootable to Different Configurations
- Clearly Not an Approved Configuration
- 2nd Hard Drive Contained Non-Maricopa County Data

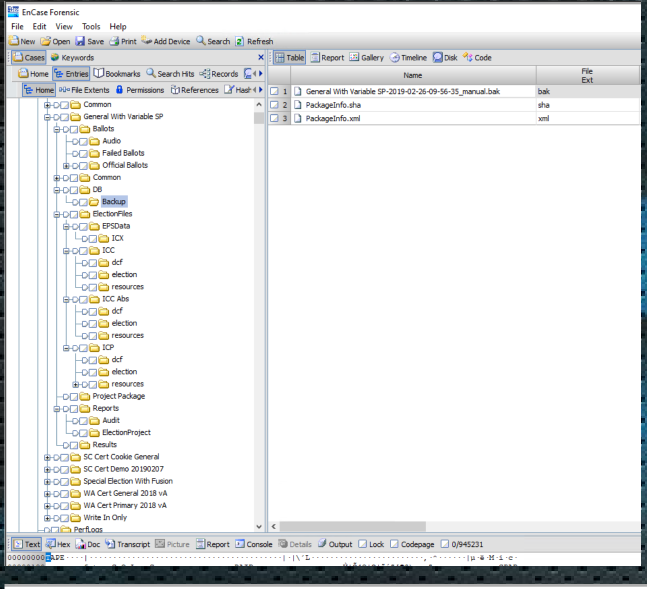


Arizona Senate Audit

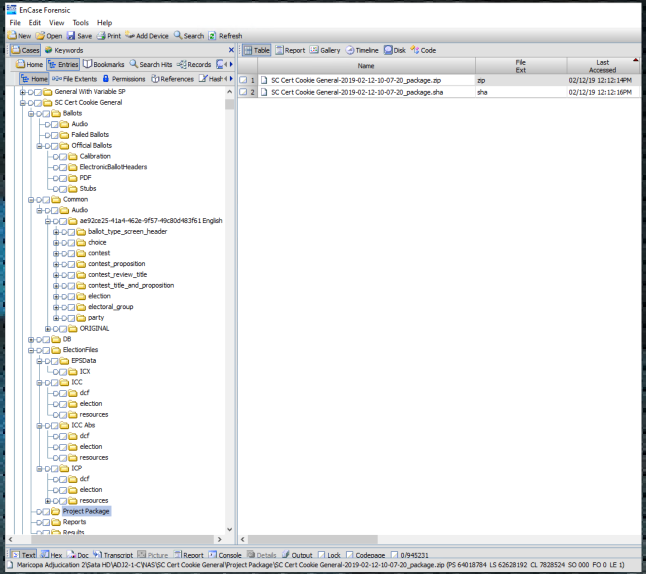
Non-Maricopa County Data



	Name	File Ext
1	bengali	
2	cantonese	
3	english	
4	french	
5	french_April_2011	
6	haitian creole	
7	icptranslations.xlsx	xlsx
8	icptranslations.xlsx.dsfx	dsfx
9	korean	
10	mandarin	
11	spanish	

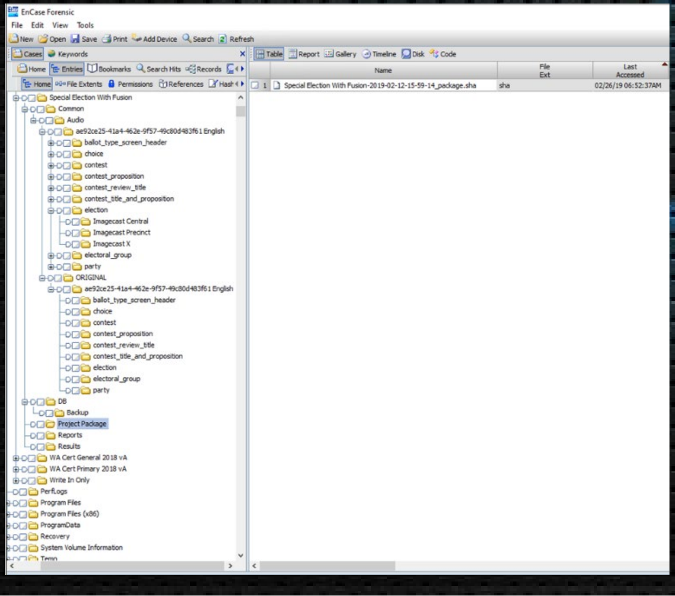


	Name	File Ext
1	General With Variable SP-2019-02-26-09-56-35_manual.bak	bak
2	PackageInfo.sha	sha
3	PackageInfo.xml	xml

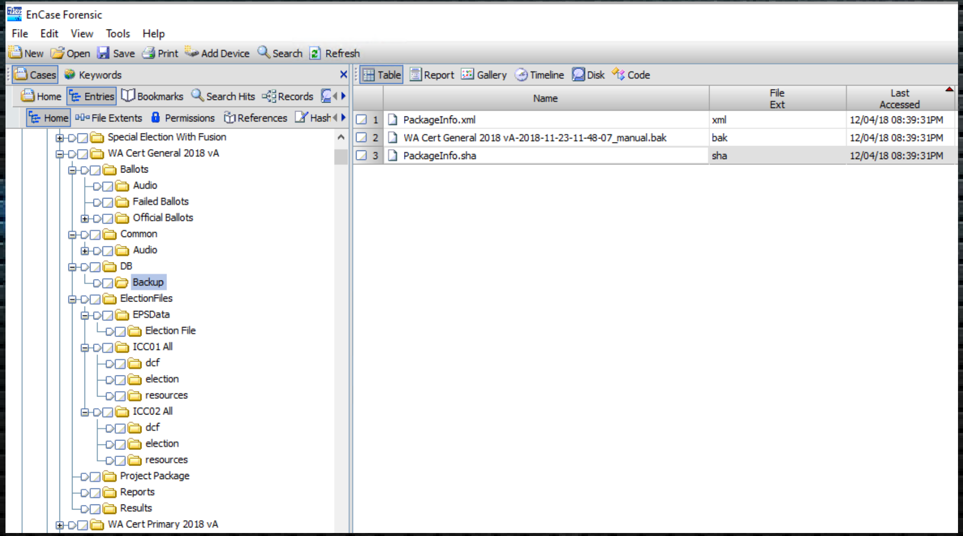


	Name	File Ext	Last Accessed
1	SC Cert Cookie General-2019-02-12-10-07-20_package.zip	zip	02/12/19 12:12:14PM
2	SC Cert Cookie General-2019-02-12-10-07-20_package.sha	sha	02/12/19 12:12:16PM

Maricopa Adjucication 2\Sata HD\ADJ2-1-C\NAS\SC Cert Cookie General\Project Package\SC Cert Cookie General-2019-02-12-10-07-20_package.zip (PS 64018784 LS 62628192 CL 7828524 SO 000 FO 0 LE 1)



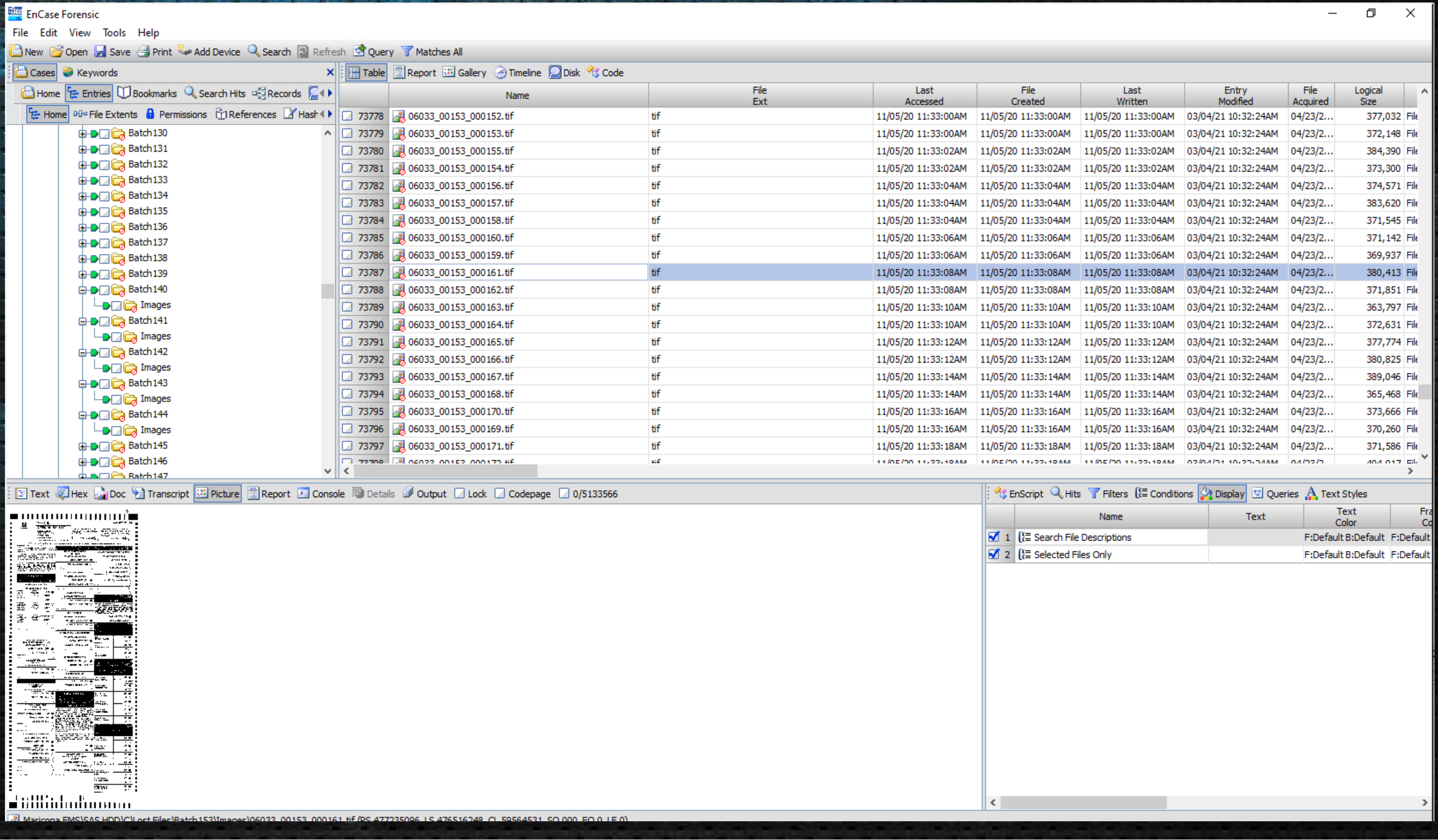
	Name	File Ext	Last Accessed
1	Special Election With Fusion-2019-02-12-15-59-14_package.sha	sha	02/26/19 06:52:37AM



	Name	File Ext	Last Accessed
1	PackageInfo.xml	xml	12/04/18 08:39:31PM
2	WA Cert General 2018 vA-2018-11-23-11-48-07_manual.bak	bak	12/04/18 08:39:31PM
3	PackageInfo.sha	sha	12/04/18 08:39:31PM

File Deletions From EMS C:\ Drive

- 865 directories and 85,673 Election Related Files (scanned ballots, .dvd files, slog.txt files, etc) Deleted Between 10/28/20 and 11/05/20



	Name	File Ext	Last Accessed	File Created	Last Written	Entry Modified	File Acquired	Logical Size	
73778	06033_00153_000152.tif	tif	11/05/20 11:33:00AM	11/05/20 11:33:00AM	11/05/20 11:33:00AM	03/04/21 10:32:24AM	04/23/2...	377,032	File
73779	06033_00153_000153.tif	tif	11/05/20 11:33:00AM	11/05/20 11:33:00AM	11/05/20 11:33:00AM	03/04/21 10:32:24AM	04/23/2...	372,148	File
73780	06033_00153_000155.tif	tif	11/05/20 11:33:02AM	11/05/20 11:33:02AM	11/05/20 11:33:02AM	03/04/21 10:32:24AM	04/23/2...	384,390	File
73781	06033_00153_000154.tif	tif	11/05/20 11:33:02AM	11/05/20 11:33:02AM	11/05/20 11:33:02AM	03/04/21 10:32:24AM	04/23/2...	373,300	File
73782	06033_00153_000156.tif	tif	11/05/20 11:33:04AM	11/05/20 11:33:04AM	11/05/20 11:33:04AM	03/04/21 10:32:24AM	04/23/2...	374,571	File
73783	06033_00153_000157.tif	tif	11/05/20 11:33:04AM	11/05/20 11:33:04AM	11/05/20 11:33:04AM	03/04/21 10:32:24AM	04/23/2...	383,620	File
73784	06033_00153_000158.tif	tif	11/05/20 11:33:04AM	11/05/20 11:33:04AM	11/05/20 11:33:04AM	03/04/21 10:32:24AM	04/23/2...	371,545	File
73785	06033_00153_000160.tif	tif	11/05/20 11:33:06AM	11/05/20 11:33:06AM	11/05/20 11:33:06AM	03/04/21 10:32:24AM	04/23/2...	371,142	File
73786	06033_00153_000159.tif	tif	11/05/20 11:33:06AM	11/05/20 11:33:06AM	11/05/20 11:33:06AM	03/04/21 10:32:24AM	04/23/2...	369,937	File
73787	06033_00153_000161.tif	tif	11/05/20 11:33:08AM	11/05/20 11:33:08AM	11/05/20 11:33:08AM	03/04/21 10:32:24AM	04/23/2...	380,413	File
73788	06033_00153_000162.tif	tif	11/05/20 11:33:08AM	11/05/20 11:33:08AM	11/05/20 11:33:08AM	03/04/21 10:32:24AM	04/23/2...	371,851	File
73789	06033_00153_000163.tif	tif	11/05/20 11:33:10AM	11/05/20 11:33:10AM	11/05/20 11:33:10AM	03/04/21 10:32:24AM	04/23/2...	363,797	File
73790	06033_00153_000164.tif	tif	11/05/20 11:33:10AM	11/05/20 11:33:10AM	11/05/20 11:33:10AM	03/04/21 10:32:24AM	04/23/2...	372,631	File
73791	06033_00153_000165.tif	tif	11/05/20 11:33:12AM	11/05/20 11:33:12AM	11/05/20 11:33:12AM	03/04/21 10:32:24AM	04/23/2...	377,774	File
73792	06033_00153_000166.tif	tif	11/05/20 11:33:12AM	11/05/20 11:33:12AM	11/05/20 11:33:12AM	03/04/21 10:32:24AM	04/23/2...	380,825	File
73793	06033_00153_000167.tif	tif	11/05/20 11:33:14AM	11/05/20 11:33:14AM	11/05/20 11:33:14AM	03/04/21 10:32:24AM	04/23/2...	389,046	File
73794	06033_00153_000168.tif	tif	11/05/20 11:33:14AM	11/05/20 11:33:14AM	11/05/20 11:33:14AM	03/04/21 10:32:24AM	04/23/2...	365,468	File
73795	06033_00153_000170.tif	tif	11/05/20 11:33:16AM	11/05/20 11:33:16AM	11/05/20 11:33:16AM	03/04/21 10:32:24AM	04/23/2...	373,666	File
73796	06033_00153_000169.tif	tif	11/05/20 11:33:16AM	11/05/20 11:33:16AM	11/05/20 11:33:16AM	03/04/21 10:32:24AM	04/23/2...	370,260	File
73797	06033_00153_000171.tif	tif	11/05/20 11:33:18AM	11/05/20 11:33:18AM	11/05/20 11:33:18AM	03/04/21 10:32:24AM	04/23/2...	371,586	File
73798	06033_00153_000172.tif	tif	11/05/20 11:33:18AM	11/05/20 11:33:18AM	11/05/20 11:33:18AM	03/04/21 10:32:24AM	04/23/2...	404,917	File

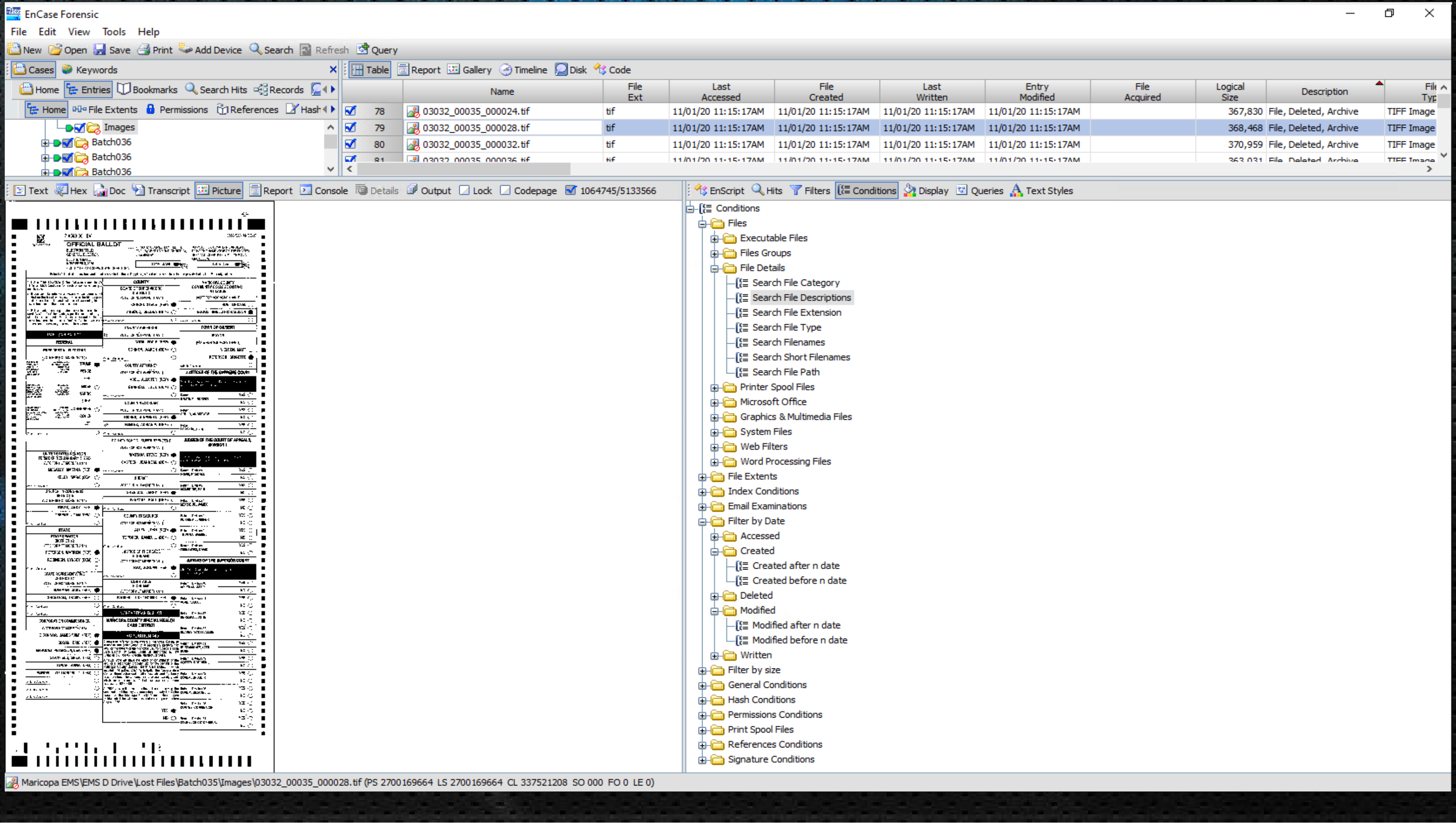
		Name	Text	Text Color	Fra Co
☑	1	Search File Descriptions		F:Default B:Default	F:Default
☑	2	Selected Files Only		F:Default B:Default	F:Default

Maricopa EMS\SAS HDD\C\Lost Files\Batch153\Images\06033_00153_000161.tif (PS 477235096 LS 476516248 CL 59564531 SO 000 FO 0 LE 0)

Arizona Senate Audit

File Deletions EMS D:\ Drive

- 9,571 Directories and 1,064,746 Election Related Files Were Deleted Between 11/01/20 and 03/16/21



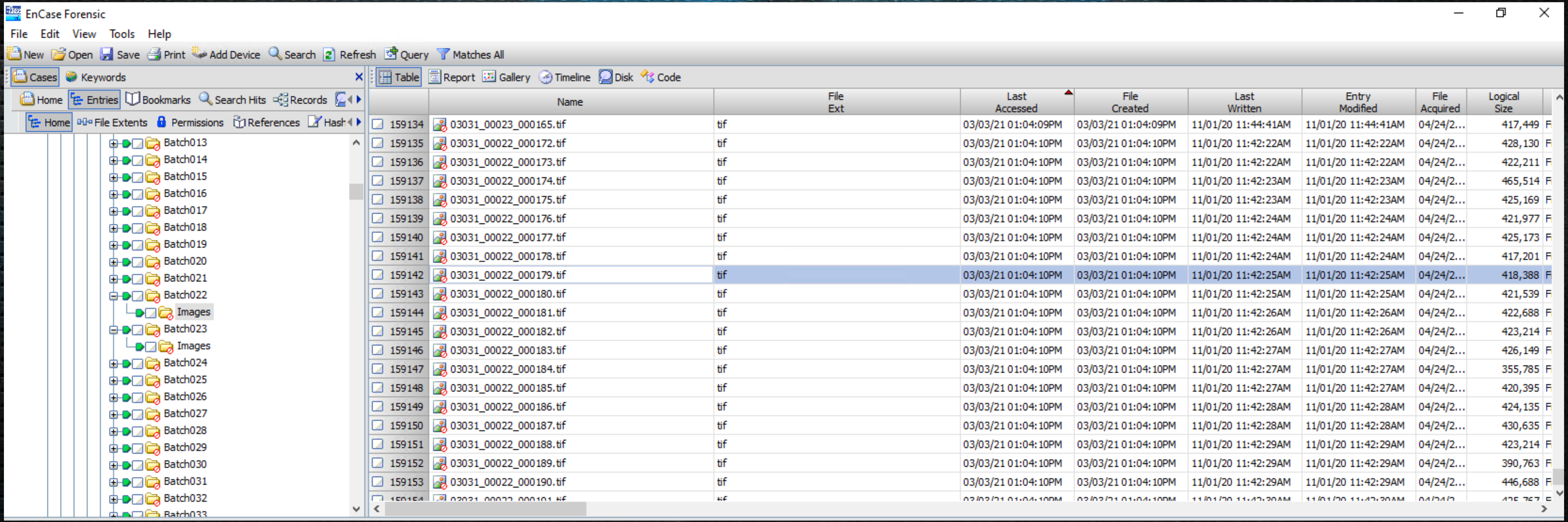
		Name	File Ext	Last Accessed	File Created	Last Written	Entry Modified	File Acquired	Logical Size	Description	File Typ
☑	78	03032_00035_000024.tif	tif	11/01/20 11:15:17AM	11/01/20 11:15:17AM	11/01/20 11:15:17AM	11/01/20 11:15:17AM		367,830	File, Deleted, Archive	TIFF Image
☑	79	03032_00035_000028.tif	tif	11/01/20 11:15:17AM	11/01/20 11:15:17AM	11/01/20 11:15:17AM	11/01/20 11:15:17AM		368,468	File, Deleted, Archive	TIFF Image
☑	80	03032_00035_000032.tif	tif	11/01/20 11:15:17AM	11/01/20 11:15:17AM	11/01/20 11:15:17AM	11/01/20 11:15:17AM		370,959	File, Deleted, Archive	TIFF Image
☑	81	03032_00035_000036.tif	tif	11/01/20 11:15:17AM	11/01/20 11:15:17AM	11/01/20 11:15:17AM	11/01/20 11:15:17AM		363,031	File, Deleted, Archive	TIFF Image

Maricopa EMS\EMS D Drive\Lost Files\Batch035\Images\03032_00035_000028.tif (PS 2700169664 LS 2700169664 CL 337521208 SO 000 FO 0 LE 0)

Arizona Senate Audit

Deleted Files – HiPro 1

- 304 Directories and 59,387 Files Containing Election Data Deleted From the HiPro Scanner 1 on 3 March 2021


EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh Query Matches All
Cases Keywords
Home Entries Bookmarks Search Hits Records
Home File Extents Permissions References Hash
Table Report Gallery Timeline Disk Code

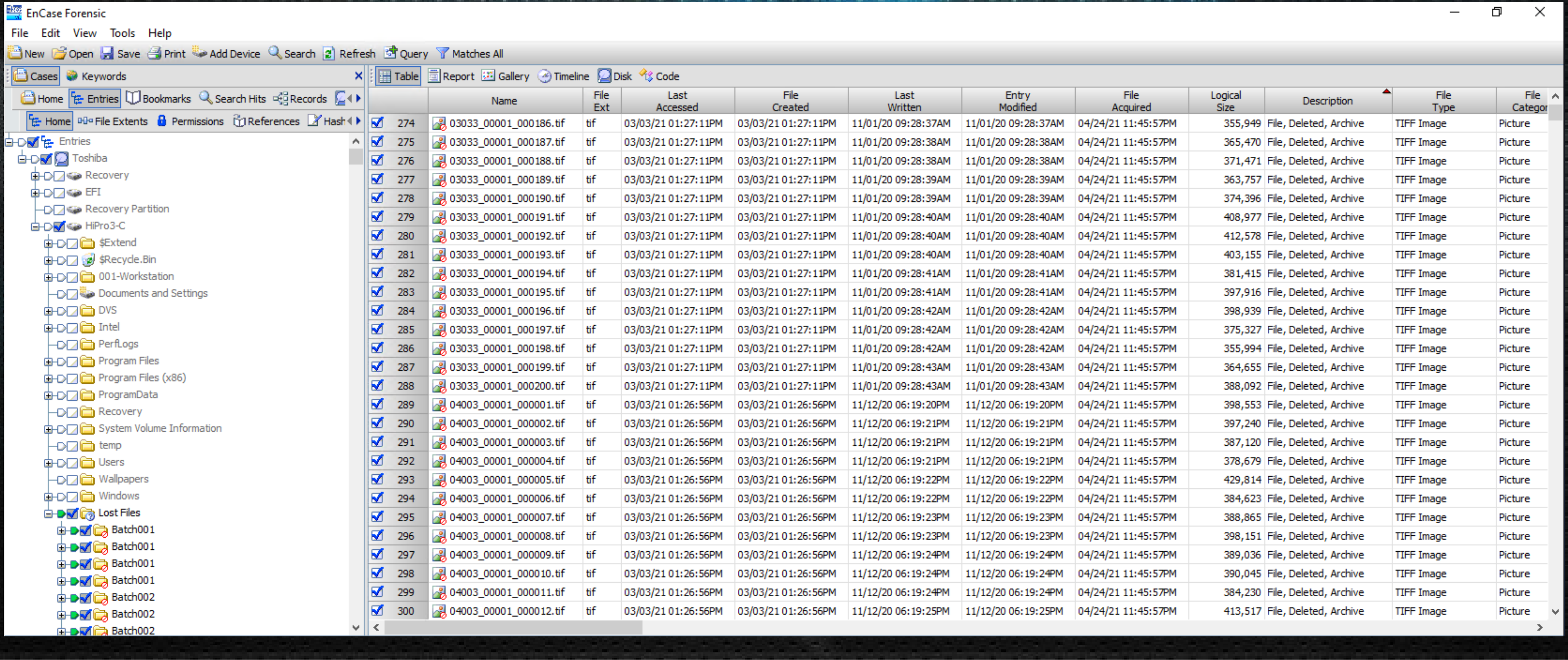
- Batch013
- Batch014
- Batch015
- Batch016
- Batch017
- Batch018
- Batch019
- Batch020
- Batch021
- Batch022
  - Images
- Batch023
  - Images
- Batch024
- Batch025
- Batch026
- Batch027
- Batch028
- Batch029
- Batch030
- Batch031
- Batch032
- Batch033

	Name	File Ext	Last Accessed	File Created	Last Written	Entry Modified	File Acquired	Logical Size	
159134	03031_00023_000165.tif	tif	03/03/21 01:04:09PM	03/03/21 01:04:09PM	11/01/20 11:44:41AM	11/01/20 11:44:41AM	04/24/2...	417,449	F
159135	03031_00022_000172.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:22AM	11/01/20 11:42:22AM	04/24/2...	428,130	F
159136	03031_00022_000173.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:22AM	11/01/20 11:42:22AM	04/24/2...	422,211	F
159137	03031_00022_000174.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:23AM	11/01/20 11:42:23AM	04/24/2...	465,514	F
159138	03031_00022_000175.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:23AM	11/01/20 11:42:23AM	04/24/2...	425,169	F
159139	03031_00022_000176.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:24AM	11/01/20 11:42:24AM	04/24/2...	421,977	F
159140	03031_00022_000177.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:24AM	11/01/20 11:42:24AM	04/24/2...	425,173	F
159141	03031_00022_000178.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:24AM	11/01/20 11:42:24AM	04/24/2...	417,201	F
159142	03031_00022_000179.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:25AM	11/01/20 11:42:25AM	04/24/2...	418,388	F
159143	03031_00022_000180.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:25AM	11/01/20 11:42:25AM	04/24/2...	421,539	F
159144	03031_00022_000181.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:26AM	11/01/20 11:42:26AM	04/24/2...	422,688	F
159145	03031_00022_000182.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:26AM	11/01/20 11:42:26AM	04/24/2...	423,214	F
159146	03031_00022_000183.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:27AM	11/01/20 11:42:27AM	04/24/2...	426,149	F
159147	03031_00022_000184.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:27AM	11/01/20 11:42:27AM	04/24/2...	355,785	F
159148	03031_00022_000185.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:27AM	11/01/20 11:42:27AM	04/24/2...	420,395	F
159149	03031_00022_000186.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:28AM	11/01/20 11:42:28AM	04/24/2...	424,135	F
159150	03031_00022_000187.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:28AM	11/01/20 11:42:28AM	04/24/2...	430,635	F
159151	03031_00022_000188.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:29AM	11/01/20 11:42:29AM	04/24/2...	423,214	F
159152	03031_00022_000189.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:29AM	11/01/20 11:42:29AM	04/24/2...	390,763	F
159153	03031_00022_000190.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:29AM	11/01/20 11:42:29AM	04/24/2...	446,688	F
159154	03031_00022_000191.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:30AM	11/01/20 11:42:30AM	04/24/2...	425,767	F

Arizona Senate Audit

Deleted Files – HiPro 3

- 1,016 Directories and 196,463 Files Containing Election Data Deleted From the HiPro Scanner 3 on 3 March 2021

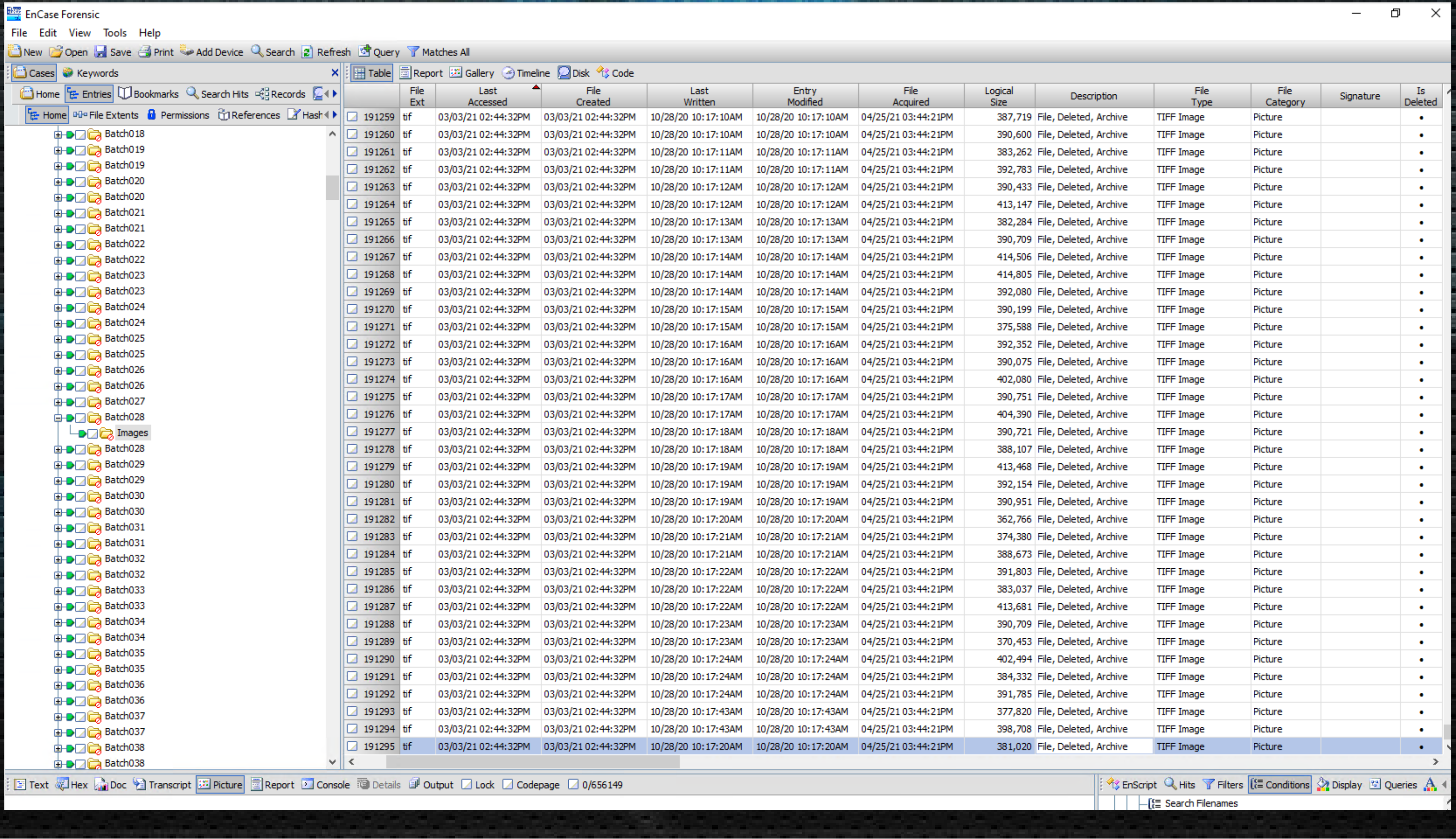


		Name	File Ext	Last Accessed	File Created	Last Written	Entry Modified	File Acquired	Logical Size	Description	File Type	File Categor
☑	274	03033_00001_000186.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:37AM	11/01/20 09:28:37AM	04/24/21 11:45:57PM	355,949	File, Deleted, Archive	TIFF Image	Picture
☑	275	03033_00001_000187.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:38AM	11/01/20 09:28:38AM	04/24/21 11:45:57PM	365,470	File, Deleted, Archive	TIFF Image	Picture
☑	276	03033_00001_000188.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:38AM	11/01/20 09:28:38AM	04/24/21 11:45:57PM	371,471	File, Deleted, Archive	TIFF Image	Picture
☑	277	03033_00001_000189.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:39AM	11/01/20 09:28:39AM	04/24/21 11:45:57PM	363,757	File, Deleted, Archive	TIFF Image	Picture
☑	278	03033_00001_000190.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:39AM	11/01/20 09:28:39AM	04/24/21 11:45:57PM	374,396	File, Deleted, Archive	TIFF Image	Picture
☑	279	03033_00001_000191.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:40AM	11/01/20 09:28:40AM	04/24/21 11:45:57PM	408,977	File, Deleted, Archive	TIFF Image	Picture
☑	280	03033_00001_000192.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:40AM	11/01/20 09:28:40AM	04/24/21 11:45:57PM	412,578	File, Deleted, Archive	TIFF Image	Picture
☑	281	03033_00001_000193.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:40AM	11/01/20 09:28:40AM	04/24/21 11:45:57PM	403,155	File, Deleted, Archive	TIFF Image	Picture
☑	282	03033_00001_000194.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:41AM	11/01/20 09:28:41AM	04/24/21 11:45:57PM	381,415	File, Deleted, Archive	TIFF Image	Picture
☑	283	03033_00001_000195.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:41AM	11/01/20 09:28:41AM	04/24/21 11:45:57PM	397,916	File, Deleted, Archive	TIFF Image	Picture
☑	284	03033_00001_000196.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:42AM	11/01/20 09:28:42AM	04/24/21 11:45:57PM	398,939	File, Deleted, Archive	TIFF Image	Picture
☑	285	03033_00001_000197.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:42AM	11/01/20 09:28:42AM	04/24/21 11:45:57PM	375,327	File, Deleted, Archive	TIFF Image	Picture
☑	286	03033_00001_000198.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:42AM	11/01/20 09:28:42AM	04/24/21 11:45:57PM	355,994	File, Deleted, Archive	TIFF Image	Picture
☑	287	03033_00001_000199.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:43AM	11/01/20 09:28:43AM	04/24/21 11:45:57PM	364,655	File, Deleted, Archive	TIFF Image	Picture
☑	288	03033_00001_000200.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:43AM	11/01/20 09:28:43AM	04/24/21 11:45:57PM	388,092	File, Deleted, Archive	TIFF Image	Picture
☑	289	04003_00001_000001.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:20PM	11/12/20 06:19:20PM	04/24/21 11:45:57PM	398,553	File, Deleted, Archive	TIFF Image	Picture
☑	290	04003_00001_000002.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:21PM	11/12/20 06:19:21PM	04/24/21 11:45:57PM	397,240	File, Deleted, Archive	TIFF Image	Picture
☑	291	04003_00001_000003.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:21PM	11/12/20 06:19:21PM	04/24/21 11:45:57PM	387,120	File, Deleted, Archive	TIFF Image	Picture
☑	292	04003_00001_000004.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:21PM	11/12/20 06:19:21PM	04/24/21 11:45:57PM	378,679	File, Deleted, Archive	TIFF Image	Picture
☑	293	04003_00001_000005.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:22PM	11/12/20 06:19:22PM	04/24/21 11:45:57PM	429,814	File, Deleted, Archive	TIFF Image	Picture
☑	294	04003_00001_000006.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:22PM	11/12/20 06:19:22PM	04/24/21 11:45:57PM	384,623	File, Deleted, Archive	TIFF Image	Picture
☑	295	04003_00001_000007.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:23PM	11/12/20 06:19:23PM	04/24/21 11:45:57PM	388,865	File, Deleted, Archive	TIFF Image	Picture
☑	296	04003_00001_000008.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:23PM	11/12/20 06:19:23PM	04/24/21 11:45:57PM	398,151	File, Deleted, Archive	TIFF Image	Picture
☑	297	04003_00001_000009.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:24PM	11/12/20 06:19:24PM	04/24/21 11:45:57PM	389,036	File, Deleted, Archive	TIFF Image	Picture
☑	298	04003_00001_000010.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:24PM	11/12/20 06:19:24PM	04/24/21 11:45:57PM	390,045	File, Deleted, Archive	TIFF Image	Picture
☑	299	04003_00001_000011.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:24PM	11/12/20 06:19:24PM	04/24/21 11:45:57PM	384,230	File, Deleted, Archive	TIFF Image	Picture
☑	300	04003_00001_000012.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:25PM	11/12/20 06:19:25PM	04/24/21 11:45:57PM	413,517	File, Deleted, Archive	TIFF Image	Picture

Arizona Senate Audit

Deleted Files – HiPro 4

- 981 Directories and 191,295 Files Containing Election Data Deleted From the HiPro Scanner 4 on 3 March 2021



	File Ext	Last Accessed	File Created	Last Written	Entry Modified	File Acquired	Logical Size	Description	File Type	File Category	Signature	Is Deleted
191259	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:10AM	10/28/20 10:17:10AM	04/25/21 03:44:21PM	387,719	File, Deleted, Archive	TIFF Image	Picture		•
191260	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:10AM	10/28/20 10:17:10AM	04/25/21 03:44:21PM	390,600	File, Deleted, Archive	TIFF Image	Picture		•
191261	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:11AM	10/28/20 10:17:11AM	04/25/21 03:44:21PM	383,262	File, Deleted, Archive	TIFF Image	Picture		•
191262	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:11AM	10/28/20 10:17:11AM	04/25/21 03:44:21PM	392,783	File, Deleted, Archive	TIFF Image	Picture		•
191263	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:12AM	10/28/20 10:17:12AM	04/25/21 03:44:21PM	390,433	File, Deleted, Archive	TIFF Image	Picture		•
191264	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:12AM	10/28/20 10:17:12AM	04/25/21 03:44:21PM	413,147	File, Deleted, Archive	TIFF Image	Picture		•
191265	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:13AM	10/28/20 10:17:13AM	04/25/21 03:44:21PM	382,284	File, Deleted, Archive	TIFF Image	Picture		•
191266	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:13AM	10/28/20 10:17:13AM	04/25/21 03:44:21PM	390,709	File, Deleted, Archive	TIFF Image	Picture		•
191267	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:14AM	10/28/20 10:17:14AM	04/25/21 03:44:21PM	414,506	File, Deleted, Archive	TIFF Image	Picture		•
191268	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:14AM	10/28/20 10:17:14AM	04/25/21 03:44:21PM	414,805	File, Deleted, Archive	TIFF Image	Picture		•
191269	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:14AM	10/28/20 10:17:14AM	04/25/21 03:44:21PM	392,080	File, Deleted, Archive	TIFF Image	Picture		•
191270	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:15AM	10/28/20 10:17:15AM	04/25/21 03:44:21PM	390,199	File, Deleted, Archive	TIFF Image	Picture		•
191271	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:15AM	10/28/20 10:17:15AM	04/25/21 03:44:21PM	375,588	File, Deleted, Archive	TIFF Image	Picture		•
191272	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:16AM	10/28/20 10:17:16AM	04/25/21 03:44:21PM	392,352	File, Deleted, Archive	TIFF Image	Picture		•
191273	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:16AM	10/28/20 10:17:16AM	04/25/21 03:44:21PM	390,075	File, Deleted, Archive	TIFF Image	Picture		•
191274	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:16AM	10/28/20 10:17:16AM	04/25/21 03:44:21PM	402,080	File, Deleted, Archive	TIFF Image	Picture		•
191275	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:17AM	10/28/20 10:17:17AM	04/25/21 03:44:21PM	390,751	File, Deleted, Archive	TIFF Image	Picture		•
191276	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:17AM	10/28/20 10:17:17AM	04/25/21 03:44:21PM	404,390	File, Deleted, Archive	TIFF Image	Picture		•
191277	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:18AM	10/28/20 10:17:18AM	04/25/21 03:44:21PM	390,721	File, Deleted, Archive	TIFF Image	Picture		•
191278	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:18AM	10/28/20 10:17:18AM	04/25/21 03:44:21PM	388,107	File, Deleted, Archive	TIFF Image	Picture		•
191279	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:19AM	10/28/20 10:17:19AM	04/25/21 03:44:21PM	413,468	File, Deleted, Archive	TIFF Image	Picture		•
191280	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:19AM	10/28/20 10:17:19AM	04/25/21 03:44:21PM	392,154	File, Deleted, Archive	TIFF Image	Picture		•
191281	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:19AM	10/28/20 10:17:19AM	04/25/21 03:44:21PM	390,951	File, Deleted, Archive	TIFF Image	Picture		•
191282	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:20AM	10/28/20 10:17:20AM	04/25/21 03:44:21PM	362,766	File, Deleted, Archive	TIFF Image	Picture		•
191283	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:21AM	10/28/20 10:17:21AM	04/25/21 03:44:21PM	374,380	File, Deleted, Archive	TIFF Image	Picture		•
191284	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:21AM	10/28/20 10:17:21AM	04/25/21 03:44:21PM	388,673	File, Deleted, Archive	TIFF Image	Picture		•
191285	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:22AM	10/28/20 10:17:22AM	04/25/21 03:44:21PM	391,803	File, Deleted, Archive	TIFF Image	Picture		•
191286	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:22AM	10/28/20 10:17:22AM	04/25/21 03:44:21PM	383,037	File, Deleted, Archive	TIFF Image	Picture		•
191287	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:22AM	10/28/20 10:17:22AM	04/25/21 03:44:21PM	413,681	File, Deleted, Archive	TIFF Image	Picture		•
191288	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:23AM	10/28/20 10:17:23AM	04/25/21 03:44:21PM	390,709	File, Deleted, Archive	TIFF Image	Picture		•
191289	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:23AM	10/28/20 10:17:23AM	04/25/21 03:44:21PM	370,453	File, Deleted, Archive	TIFF Image	Picture		•
191290	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:24AM	10/28/20 10:17:24AM	04/25/21 03:44:21PM	402,494	File, Deleted, Archive	TIFF Image	Picture		•
191291	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:24AM	10/28/20 10:17:24AM	04/25/21 03:44:21PM	384,332	File, Deleted, Archive	TIFF Image	Picture		•
191292	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:24AM	10/28/20 10:17:24AM	04/25/21 03:44:21PM	391,785	File, Deleted, Archive	TIFF Image	Picture		•
191293	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:43AM	10/28/20 10:17:43AM	04/25/21 03:44:21PM	377,820	File, Deleted, Archive	TIFF Image	Picture		•
191294	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:43AM	10/28/20 10:17:43AM	04/25/21 03:44:21PM	398,708	File, Deleted, Archive	TIFF Image	Picture		•
191295	tif	03/03/21 02:44:32PM	03/03/21 02:44:32PM	10/28/20 10:17:20AM	10/28/20 10:17:20AM	04/25/21 03:44:21PM	381,020	File, Deleted, Archive	TIFF Image	Picture		•

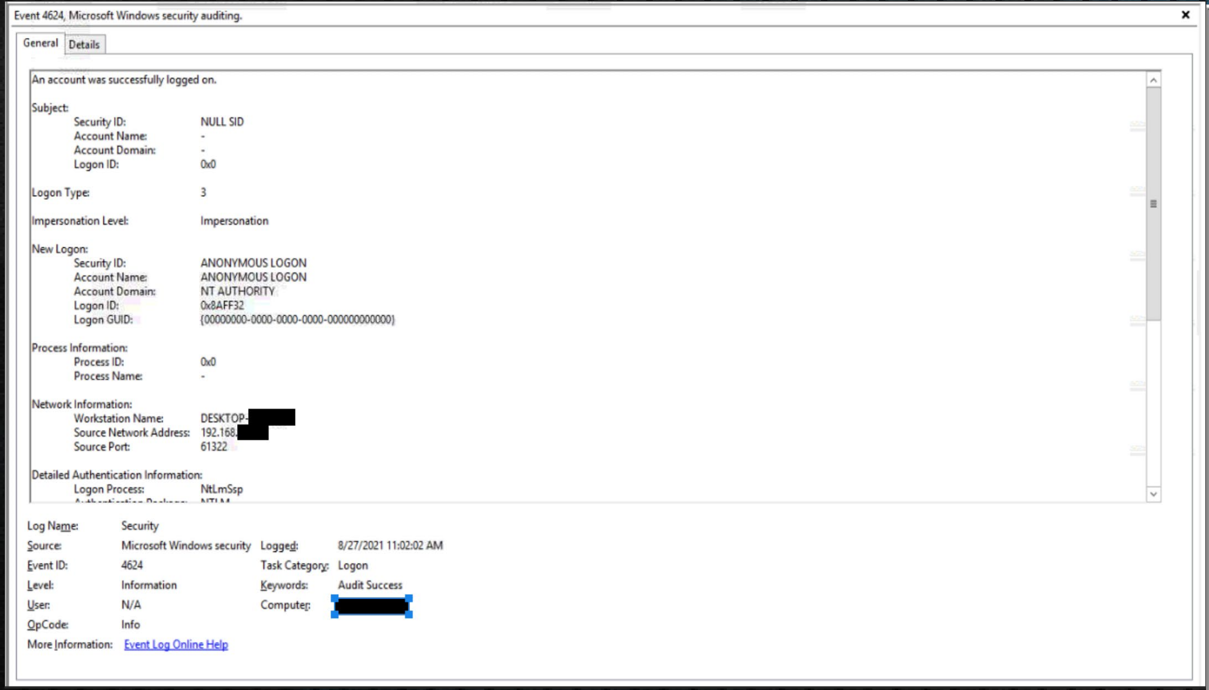
Failure to Preserve Operating System Logs

- Logs Produced by Maricopa County Did Not Contain the Windows Security Logs
- Security Logs Set to Maintain 20MB of Data
- Oldest Date in Windows Security Log on EMS was 2/5/21
  - Did not Cover Election Time Period
- Clear Intentional Overwriting of the Security Logs by the EMSADMIN Account
  - 2/11/2021 – 462 Log Entries Overwritten
  - 3/3/2021 - 37,686 Log Entries Overwritten
  - 4/12/2021 – 330 Log Entries Overwritten

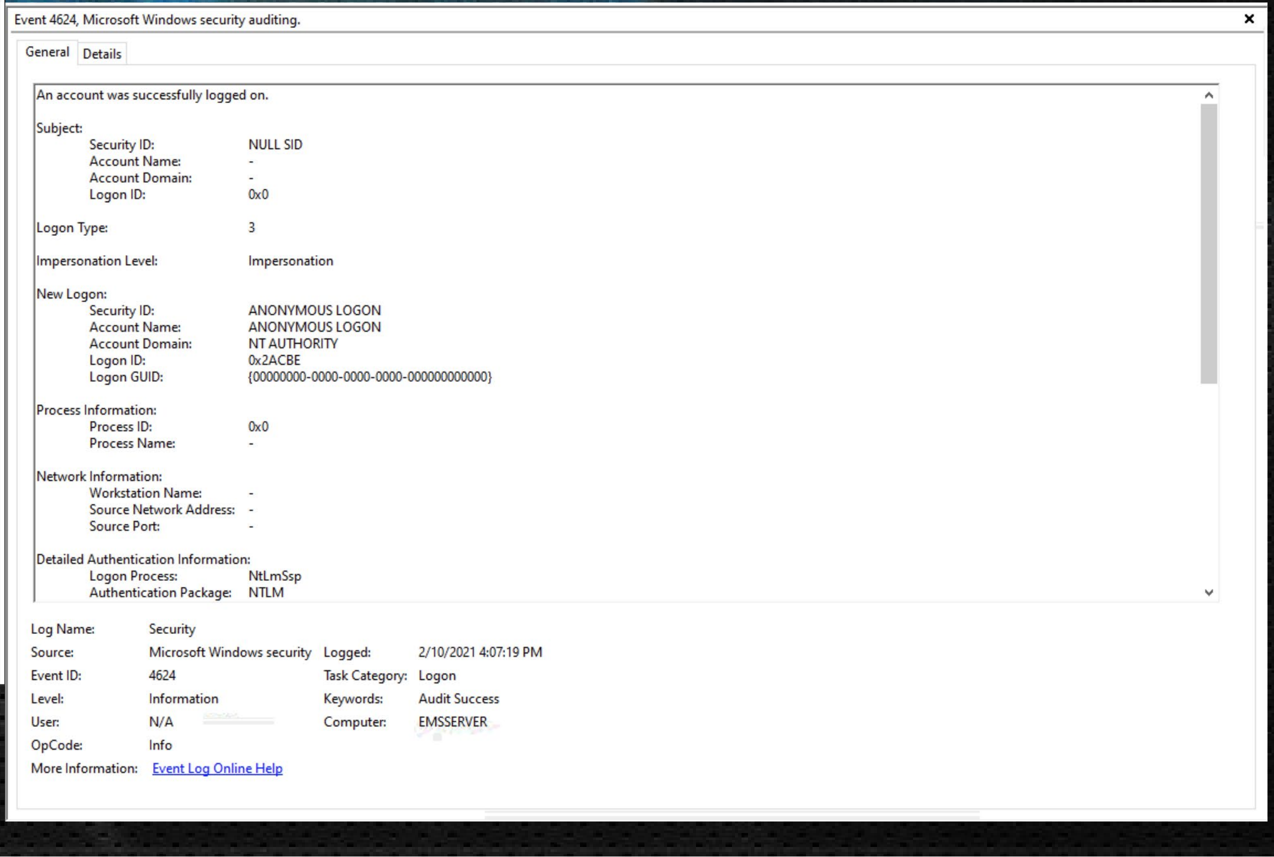
Arizona Senate Audit

Anonymous Logins

- Some Anonymous Login Activity is Normal
- Atypical Anonymous Logins Were Discovered



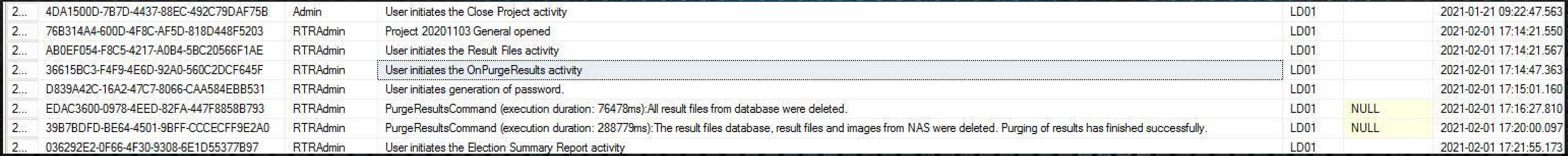
```
Event 4624, Microsoft Windows security auditing.

General | Details

An account was successfully logged on.

Subject:
        Security ID:              NULL SID
        Account Name:             -
        Account Domain:           -
        Logon ID:                 0x0

Logon Type:                       3

Impersonation Level:              Impersonation

New Logon:
        Security ID:              ANONYMOUS LOGON
        Account Name:             ANONYMOUS LOGON
        Account Domain:           NT AUTHORITY
        Logon ID:                 0x8AFF32
        Logon GUID:               {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:               0x0
        Process Name:             -

Network Information:
        Workstation Name:         DESKTOP-[redacted]
        Source Network Address:   192.168.[redacted]
        Source Port:              61322

Detailed Authentication Information:
        Logon Process:            NtLmSsp
        Authentication Package:   NTLM

Log Name:     Security
Source:       Microsoft Windows security   Logged:         8/27/2021 11:02:02 AM
Event ID:     4624                         Task Category:  Logon
Level:        Information                  Keywords:       Audit Success
User:         N/A                          Computer:       [redacted]
OpCode:       Info
More Information:  Event Log Online Help
```



```
Event 4624, Microsoft Windows security auditing.

General | Details

An account was successfully logged on.

Subject:
        Security ID:              NULL SID
        Account Name:             -
        Account Domain:           -
        Logon ID:                 0x0

Logon Type:                       3

Impersonation Level:              Impersonation

New Logon:
        Security ID:              ANONYMOUS LOGON
        Account Name:             ANONYMOUS LOGON
        Account Domain:           NT AUTHORITY
        Logon ID:                 0x2ACBE
        Logon GUID:               {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:               0x0
        Process Name:             -

Network Information:
        Workstation Name:         -
        Source Network Address:   -
        Source Port:              -

Detailed Authentication Information:
        Logon Process:            NtLmSsp
        Authentication Package:   NTLM

Log Name:     Security
Source:       Microsoft Windows security   Logged:         2/10/2021 4:07:19 PM
Event ID:     4624                         Task Category:  Logon
Level:        Information                  Keywords:       Audit Success
User:         N/A                          Computer:       EMSSERVER
OpCode:       Info
More Information:  Event Log Online Help
```

General Election Results Purged from EMS

- 2/1/2021 – SQL Logs Indicate That the RTRAdmin Account Purged the General Election Results from the Database
- Windows Access Logs Don’t have a Corresponding Entry



2...	4DA1500D-7B7D-4437-88EC-492C79DAF75B	Admin	User initiates the Close Project activity	LD01		2021-01-21 09:22:47.563
2...	76B314A4-600D-4F8C-AF5D-818D448F5203	RTRAdmin	Project 20201103 General opened	LD01		2021-02-01 17:14:21.550
2...	AB0EF054-F8C5-4217-A0B4-5BC20566F1AE	RTRAdmin	User initiates the Result Files activity	LD01		2021-02-01 17:14:21.567
2...	36615BC3-F4F9-4E6D-92A0-560C2DCF645F	RTRAdmin	User initiates the OnPurgeResults activity	LD01		2021-02-01 17:14:47.363
2...	D839A42C-16A2-47C7-8066-CAA584EBB531	RTRAdmin	User initiates generation of password.	LD01		2021-02-01 17:15:01.160
2...	EDAC3600-0978-4EED-82FA-447F8858B793	RTRAdmin	PurgeResultsCommand (execution duration: 76478ms):All result files from database were deleted.	LD01	NULL	2021-02-01 17:16:27.810
2...	39B7BDFD-BE64-4501-9BFF-CCCECFF9E2A0	RTRAdmin	PurgeResultsCommand (execution duration: 288779ms):The result files database, result files and images from NAS were deleted. Purging of results has finished successfully.	LD01	NULL	2021-02-01 17:20:00.097
2...	036292E2-0F66-4F30-9308-6E1D55377B97	RTRAdmin	User initiates the Election Summary Report activity	LD01		2021-02-01 17:21:55.173

EMS Listening Ports

- Analysis Discovered 59 Ports That Were Open on the EMS Server at Boot
- Unexpected High Port Listening Activity by Standard Windows Processes (winit.exe, dns.exe, dhcpserver)
- IPV6 Enabled
- Terminal Services are Enabled
- Remote Access is Enabled

EMS Network Connection Attempts on Boot

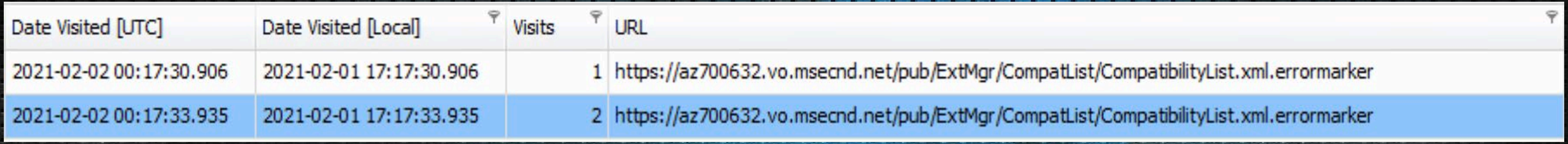
Process Name	Process File Path	Process ID	Dest IP	Dest Port	Whois
system	system	4	192.168.100.1	445	N/A Local Lan
avastsvc.exe	c:\program files\avast software\avast business\avastsvc.exe	320	23.194.212.49	80	Akamai
avastsvc.exe	c:\program files\avast software\avast business\avastsvc.exe	320	23.194.212.56	80	Akamai
svchost.exe	c:\windows\system32\svchost.exe	988	8.252.68.126	80	Level 3 Parent, LLC
svchost.exe	c:\windows\system32\svchost.exe	988	72.21.81.240	80	Edgecast
svchost.exe	c:\windows\system32\svchost.exe	988	13.107.4.50	80	Microsoft
svchost.exe	c:\windows\system32\svchost.exe	988	23.194.212.104	80	Akamai
svchost.exe	c:\windows\system32\svchost.exe	988	8.240.49.254	80	Level 3 Parent, LLC
svchost.exe	c:\windows\system32\svchost.exe	988	8.252.36.126	80	Level 3 Parent, LLC
svchost.exe	c:\windows\system32\svchost.exe	1272	64.4.54.254	443	Microsoft
svchost.exe	c:\windows\system32\svchost.exe	1272	52.137.106.217	443	Microsoft
svchost.exe	c:\windows\system32\svchost.exe	1272	20.72.205.209	443	Microsoft
jusched.exe	c:\program files (x86)\common files\java\java update\jusched.exe	4680	184.86.196.202	443	Akamai
avastemupdate.exe	c:\program files\avast software\avast business\avastemupdate.exe	8092	104.99.72.230	80	Akamai

Internet History and Connections

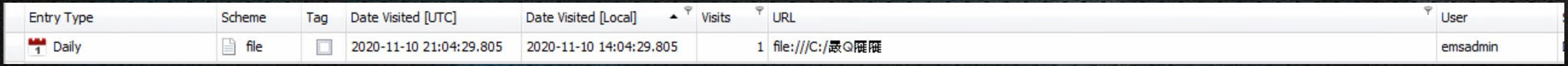
- Both Maricopa County Audits did Not Find Any Internet History
- Significant Internet History Recovered from Unallocated Space
  - EMS Server
  - EMS Client Workstations
  - Adjudication Workstations
  - REWEB 1601
  - REGIS 1202

Arizona Senate Audit

EMS Server

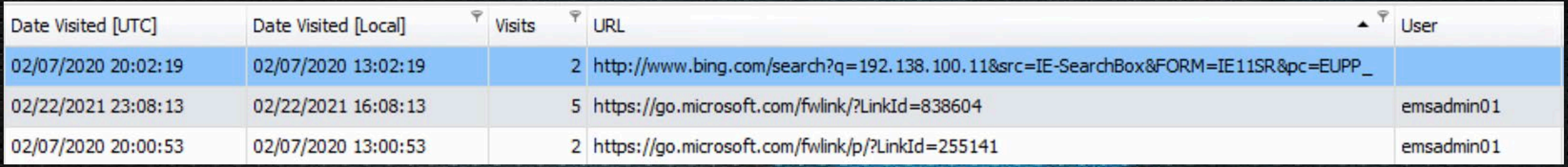


Date Visited [UTC]	Date Visited [Local]	Visits	URL
2021-02-02 00:17:30.906	2021-02-01 17:17:30.906	1	https://az700632.vo.msecnd.net/pub/ExtMgr/CompatList/CompatibilityList.xml.errormarker
2021-02-02 00:17:33.935	2021-02-01 17:17:33.935	2	https://az700632.vo.msecnd.net/pub/ExtMgr/CompatList/CompatibilityList.xml.errormarker

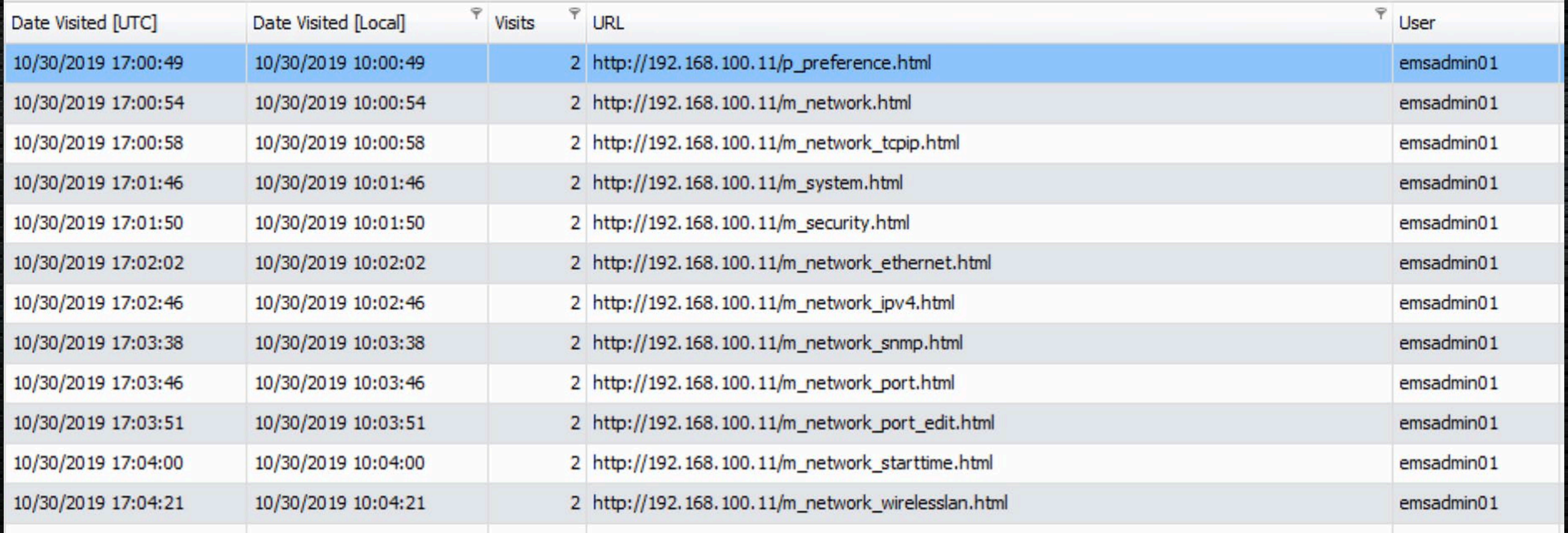


Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL	User
Daily	file	□	2020-11-10 21:04:29.805	2020-11-10 14:04:29.805	1	file:///C:/聂Q罹罹	emsadmin

EMS Client 1

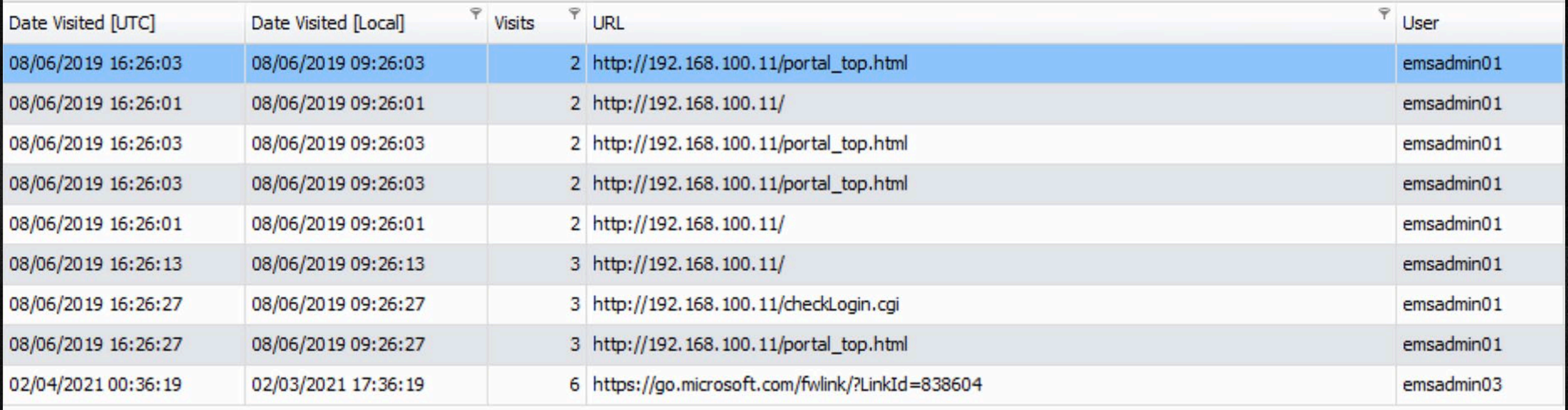


Date Visited [UTC]	Date Visited [Local]	Visits	URL	User
02/07/2020 20:02:19	02/07/2020 13:02:19	2	http://www.bing.com/search?q=192.138.100.11&src=IE-SearchBox&FORM=IE11SR&pc=EUPP_	
02/22/2021 23:08:13	02/22/2021 16:08:13	5	https://go.microsoft.com/fwlink/?LinkId=838604	emsadmin01
02/07/2020 20:00:53	02/07/2020 13:00:53	2	https://go.microsoft.com/fwlink/p/?LinkId=255141	emsadmin01



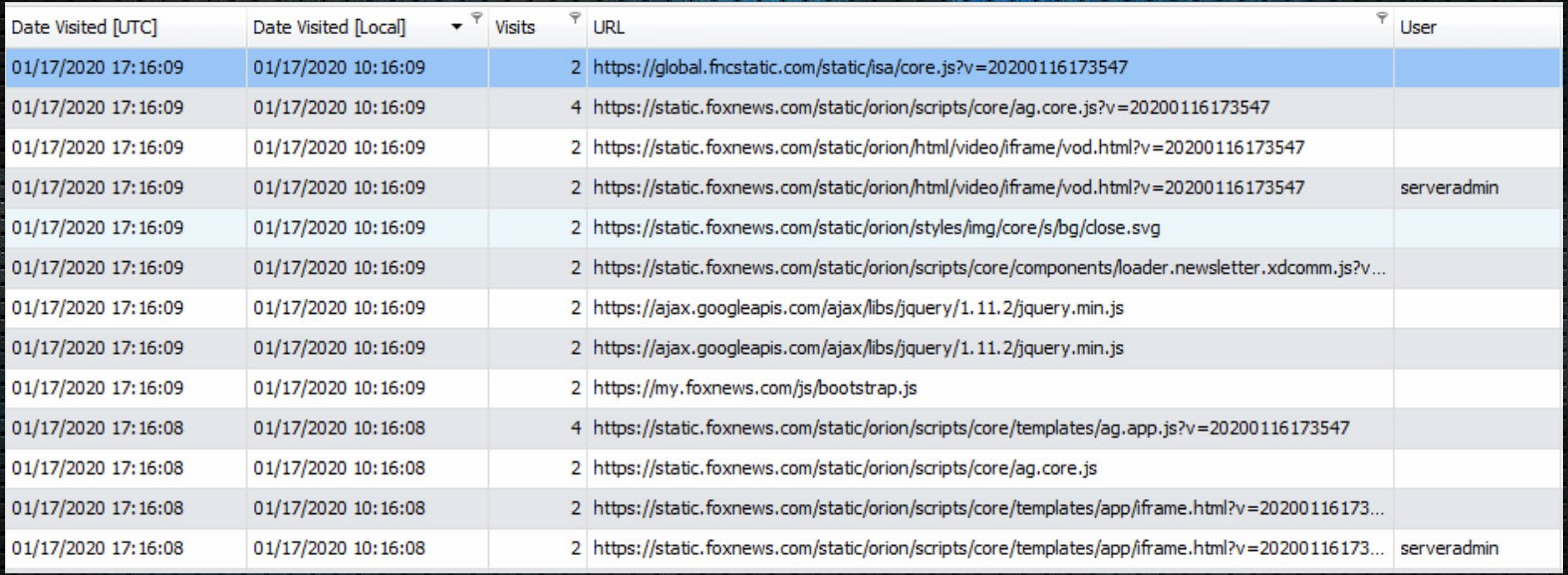
Date Visited [UTC]	Date Visited [Local]	Visits	URL	User
10/30/2019 17:00:49	10/30/2019 10:00:49	2	http://192.168.100.11/p_preference.html	emsadmin01
10/30/2019 17:00:54	10/30/2019 10:00:54	2	http://192.168.100.11/m_network.html	emsadmin01
10/30/2019 17:00:58	10/30/2019 10:00:58	2	http://192.168.100.11/m_network_tcpip.html	emsadmin01
10/30/2019 17:01:46	10/30/2019 10:01:46	2	http://192.168.100.11/m_system.html	emsadmin01
10/30/2019 17:01:50	10/30/2019 10:01:50	2	http://192.168.100.11/m_security.html	emsadmin01
10/30/2019 17:02:02	10/30/2019 10:02:02	2	http://192.168.100.11/m_network_ethernet.html	emsadmin01
10/30/2019 17:02:46	10/30/2019 10:02:46	2	http://192.168.100.11/m_network_ipv4.html	emsadmin01
10/30/2019 17:03:38	10/30/2019 10:03:38	2	http://192.168.100.11/m_network_snmp.html	emsadmin01
10/30/2019 17:03:46	10/30/2019 10:03:46	2	http://192.168.100.11/m_network_port.html	emsadmin01
10/30/2019 17:03:51	10/30/2019 10:03:51	2	http://192.168.100.11/m_network_port_edit.html	emsadmin01
10/30/2019 17:04:00	10/30/2019 10:04:00	2	http://192.168.100.11/m_network_starttime.html	emsadmin01
10/30/2019 17:04:21	10/30/2019 10:04:21	2	http://192.168.100.11/m_network_wirelesslan.html	emsadmin01

EMS Client 3



Date Visited [UTC]	Date Visited [Local]	Visits	URL	User
08/06/2019 16:26:03	08/06/2019 09:26:03	2	http://192.168.100.11/portal_top.html	emsadmin01
08/06/2019 16:26:01	08/06/2019 09:26:01	2	http://192.168.100.11/	emsadmin01
08/06/2019 16:26:03	08/06/2019 09:26:03	2	http://192.168.100.11/portal_top.html	emsadmin01
08/06/2019 16:26:03	08/06/2019 09:26:03	2	http://192.168.100.11/portal_top.html	emsadmin01
08/06/2019 16:26:01	08/06/2019 09:26:01	2	http://192.168.100.11/	emsadmin01
08/06/2019 16:26:13	08/06/2019 09:26:13	3	http://192.168.100.11/	emsadmin01
08/06/2019 16:26:27	08/06/2019 09:26:27	3	http://192.168.100.11/checkLogin.cgi	emsadmin01
08/06/2019 16:26:27	08/06/2019 09:26:27	3	http://192.168.100.11/portal_top.html	emsadmin01
02/04/2021 00:36:19	02/03/2021 17:36:19	6	https://go.microsoft.com/fwlink/?LinkId=838604	emsadmin03

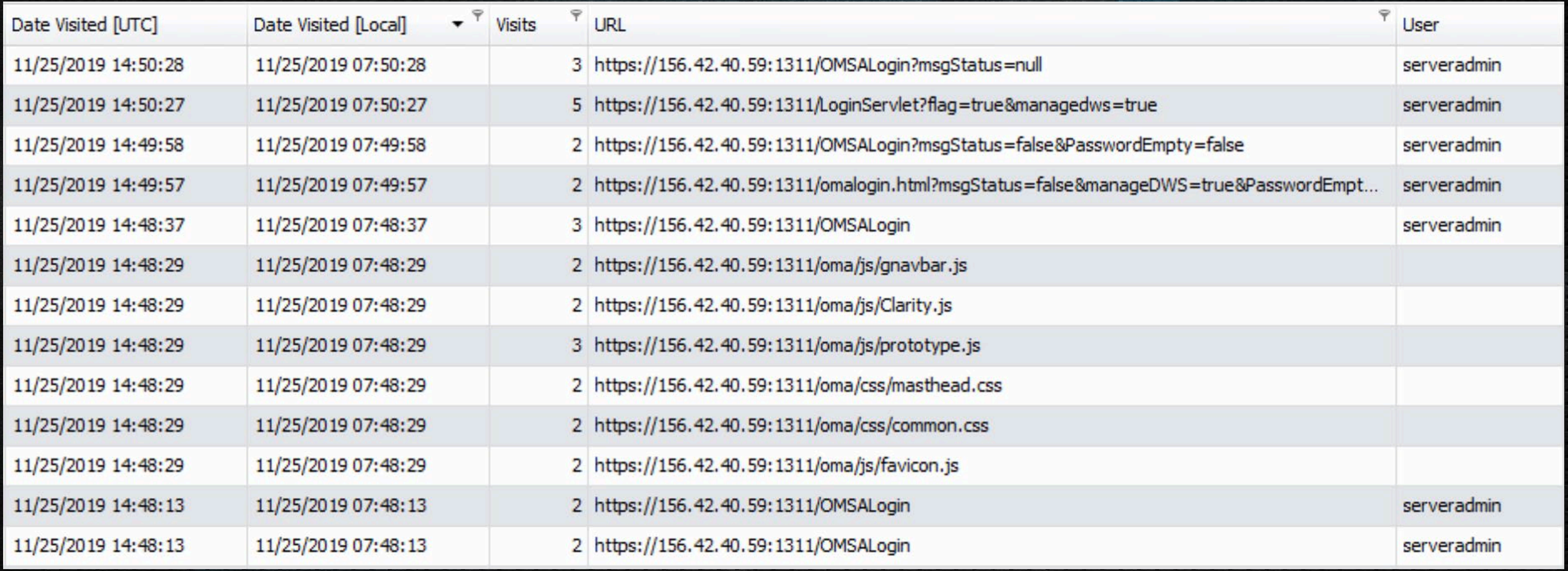
REWEB1601



Date Visited [UTC]	Date Visited [Local]	Visits	URL	User
01/17/2020 17:16:09	01/17/2020 10:16:09	2	https://global.fncstatic.com/static/isa/core.js?v=20200116173547	
01/17/2020 17:16:09	01/17/2020 10:16:09	4	https://static.foxnews.com/static/orion/scripts/core/ag.core.js?v=20200116173547	
01/17/2020 17:16:09	01/17/2020 10:16:09	2	https://static.foxnews.com/static/orion/html/video/iframe/vod.html?v=20200116173547	
01/17/2020 17:16:09	01/17/2020 10:16:09	2	https://static.foxnews.com/static/orion/html/video/iframe/vod.html?v=20200116173547	serveradmin
01/17/2020 17:16:09	01/17/2020 10:16:09	2	https://static.foxnews.com/static/orion/styles/img/core/s/bg/close.svg	
01/17/2020 17:16:09	01/17/2020 10:16:09	2	https://static.foxnews.com/static/orion/scripts/core/components/loader.newsletter.xdcomm.js?v...	
01/17/2020 17:16:09	01/17/2020 10:16:09	2	https://ajax.googleapis.com/ajax/libs/jquery/1.11.2/jquery.min.js	
01/17/2020 17:16:09	01/17/2020 10:16:09	2	https://ajax.googleapis.com/ajax/libs/jquery/1.11.2/jquery.min.js	
01/17/2020 17:16:09	01/17/2020 10:16:09	2	https://my.foxnews.com/js/bootstrap.js	
01/17/2020 17:16:08	01/17/2020 10:16:08	4	https://static.foxnews.com/static/orion/scripts/core/templates/ag.app.js?v=20200116173547	
01/17/2020 17:16:08	01/17/2020 10:16:08	2	https://static.foxnews.com/static/orion/scripts/core/ag.core.js	
01/17/2020 17:16:08	01/17/2020 10:16:08	2	https://static.foxnews.com/static/orion/scripts/core/templates/app/iframe.html?v=20200116173...	
01/17/2020 17:16:08	01/17/2020 10:16:08	2	https://static.foxnews.com/static/orion/scripts/core/templates/app/iframe.html?v=20200116173...	serveradmin
]

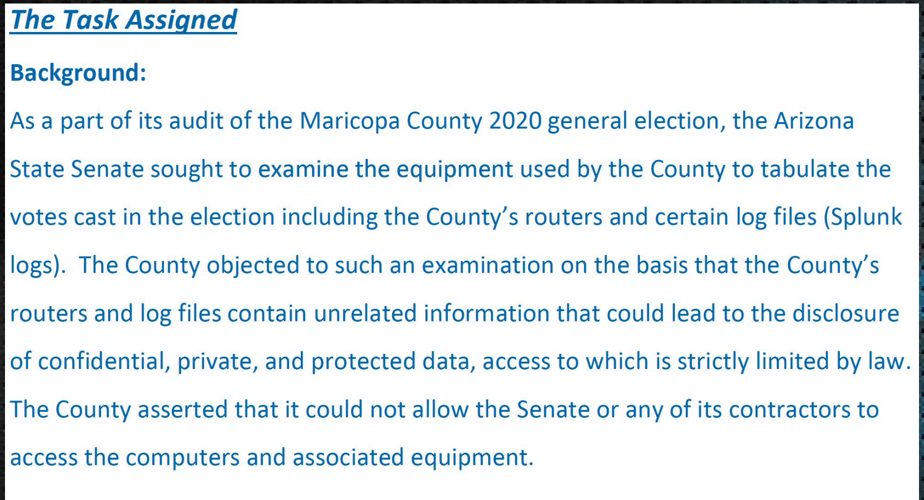
Arizona Senate Audit

REGIS 1202



Date Visited [UTC]	Date Visited [Local]	Visits	URL	User
11/25/2019 14:50:28	11/25/2019 07:50:28	3	https://156.42.40.59:1311/OMSALogin?msgStatus=null	serveradmin
11/25/2019 14:50:27	11/25/2019 07:50:27	5	https://156.42.40.59:1311/LoginServlet?flag=true&managedws=true	serveradmin
11/25/2019 14:49:58	11/25/2019 07:49:58	2	https://156.42.40.59:1311/OMSALogin?msgStatus=false&PasswordEmpty=false	serveradmin
11/25/2019 14:49:57	11/25/2019 07:49:57	2	https://156.42.40.59:1311/omalogin.html?msgStatus=false&manageDWS=true&PasswordEmpt...	serveradmin
11/25/2019 14:48:37	11/25/2019 07:48:37	3	https://156.42.40.59:1311/OMSALogin	serveradmin
11/25/2019 14:48:29	11/25/2019 07:48:29	2	https://156.42.40.59:1311/oma/js/gnavbar.js	
11/25/2019 14:48:29	11/25/2019 07:48:29	2	https://156.42.40.59:1311/oma/js/Clarity.js	
11/25/2019 14:48:29	11/25/2019 07:48:29	3	https://156.42.40.59:1311/oma/js/prototype.js	
11/25/2019 14:48:29	11/25/2019 07:48:29	2	https://156.42.40.59:1311/oma/css/masthead.css	
11/25/2019 14:48:29	11/25/2019 07:48:29	2	https://156.42.40.59:1311/oma/css/common.css	
11/25/2019 14:48:29	11/25/2019 07:48:29	2	https://156.42.40.59:1311/oma/js/favicon.js	
11/25/2019 14:48:13	11/25/2019 07:48:13	2	https://156.42.40.59:1311/OMSALogin	serveradmin
11/25/2019 14:48:13	11/25/2019 07:48:13	2	https://156.42.40.59:1311/OMSALogin	serveradmin

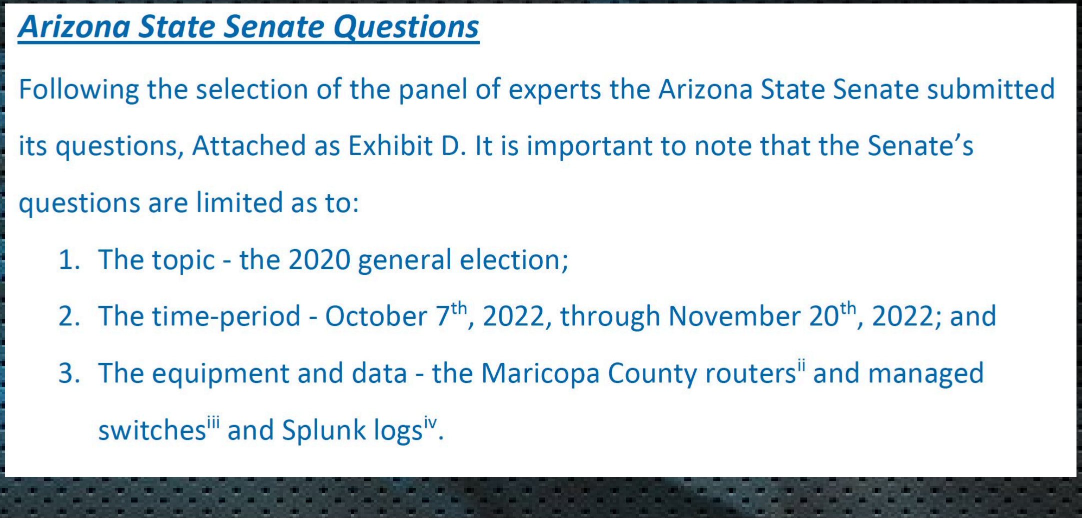
The Results of the Special Master Report are Flawed



The Task Assigned

Background:

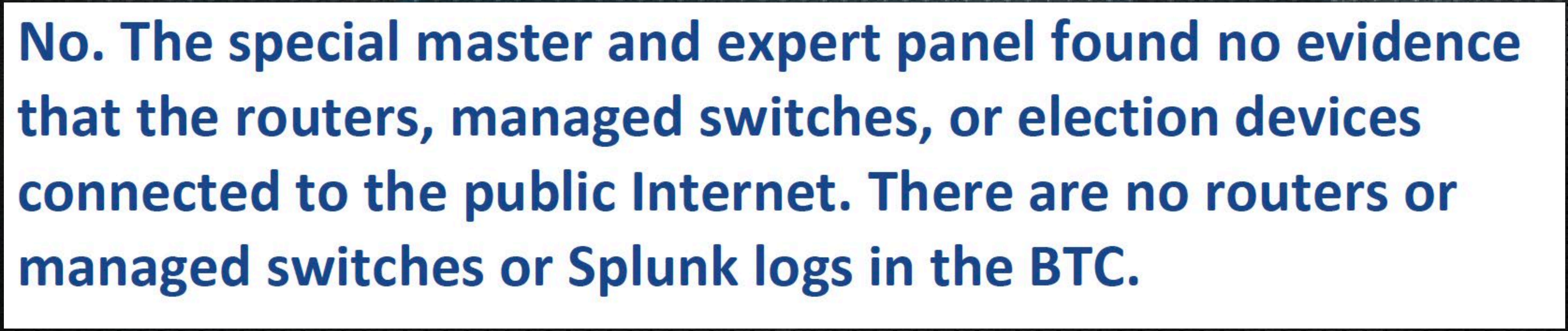
As a part of its audit of the Maricopa County 2020 general election, the Arizona State Senate sought to examine the equipment used by the County to tabulate the votes cast in the election including the County's routers and certain log files (Splunk logs). The County objected to such an examination on the basis that the County's routers and log files contain unrelated information that could lead to the disclosure of confidential, private, and protected data, access to which is strictly limited by law. The County asserted that it could not allow the Senate or any of its contractors to access the computers and associated equipment.



Arizona State Senate Questions

Following the selection of the panel of experts the Arizona State Senate submitted its questions, Attached as Exhibit D. It is important to note that the Senate's questions are limited as to:

1. The topic - the 2020 general election;
2. The time-period - October 7th, 2022, through November 20th, 2022; and
3. The equipment and data - the Maricopa County routers[ii] and managed switches[iii] and Splunk logs[iv].

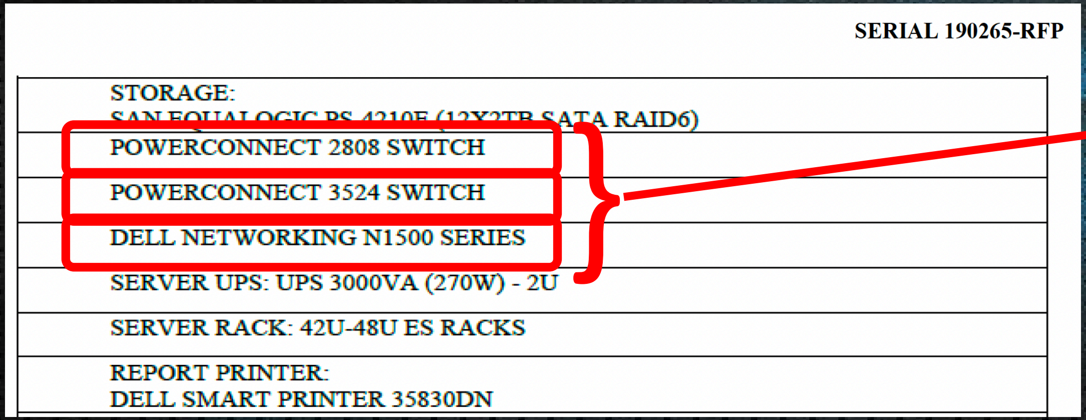


No. The special master and expert panel found no evidence that the routers, managed switches, or election devices connected to the public Internet. There are no routers or managed switches or Splunk logs in the BTC.

Arizona Senate Audit

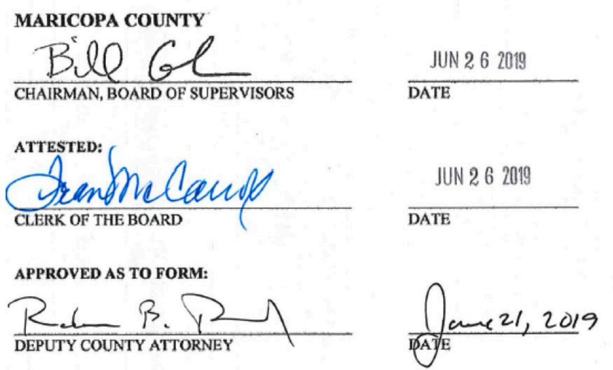
Switches and Routers

- Contract Dated 6/26/19 Page 29



SERIAL 190265-RFP

STORAGE: SAN EQUALOGIC PS 4210E (12X2TB SATA RAID6)
POWERCONNECT 2808 SWITCH
POWERCONNECT 3524 SWITCH
DELL NETWORKING N1500 SERIES
SERVER UPS: UPS 3000VA (270W) - 2U
SERVER RACK: 42U-48U ES RACKS
REPORT PRINTER: DELL SMART PRINTER 35830DN



MARICOPA COUNTY

Bill G

CHAIRMAN, BOARD OF SUPERVISORS

JUN 2 6 2019

DATE

ATTESTED:

Fran McCarroll

CLERK OF THE BOARD

JUN 2 6 2019

DATE

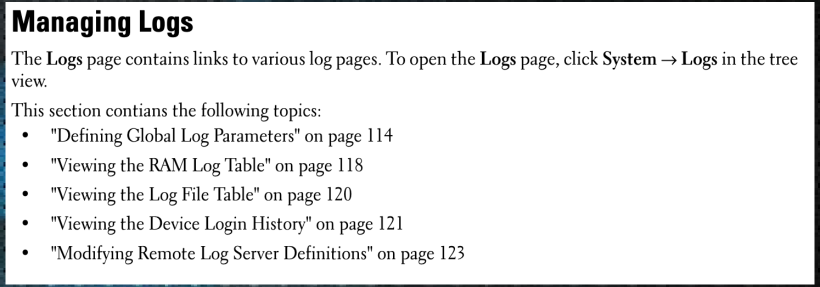
APPROVED AS TO FORM:

DEPUTY COUNTY ATTORNEY

June 21, 2019

DATE

Managed Switches

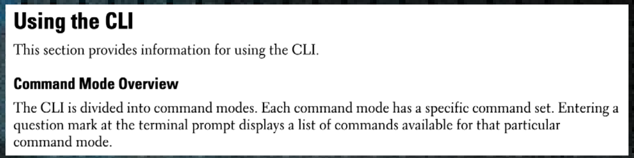


Managing Logs

The **Logs** page contains links to various log pages. To open the **Logs** page, click **System** → **Logs** in the tree view.

This section contians the following topics:

- "Defining Global Log Parameters" on page 114
- "Viewing the RAM Log Table" on page 118
- "Viewing the Log File Table" on page 120
- "Viewing the Device Login History" on page 121
- "Modifying Remote Log Server Definitions" on page 123

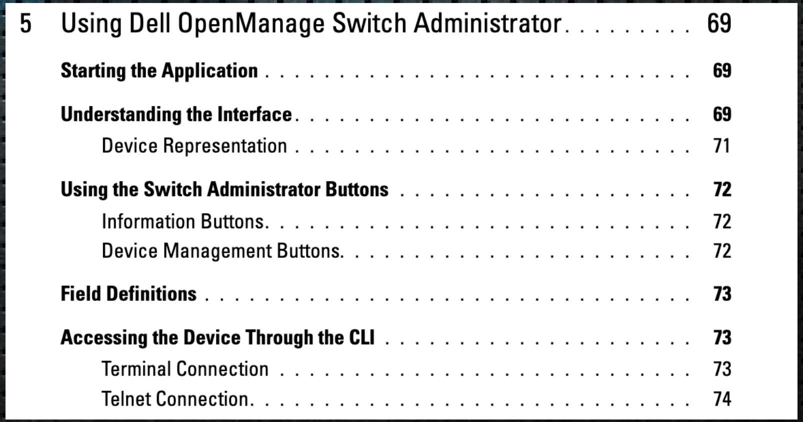


Using the CLI

This section provides information for using the CLI.

Command Mode Overview

The CLI is divided into command modes. Each command mode has a specific command set. Entering a question mark at the terminal prompt displays a list of commands available for that particular command mode.



5 Using Dell OpenManage Switch Administrator 69

Starting the Application 69

Understanding the Interface 69

Device Representation 71

Using the Switch Administrator Buttons 72

Information Buttons. 72

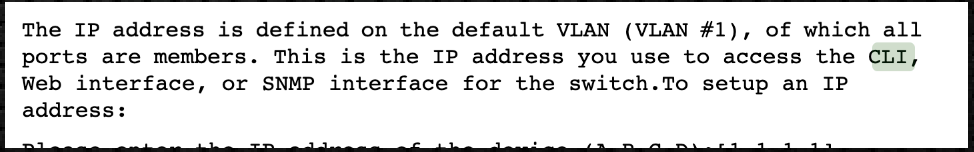
Device Management Buttons. 72

Field Definitions 73

Accessing the Device Through the CLI 73

Terminal Connection 73

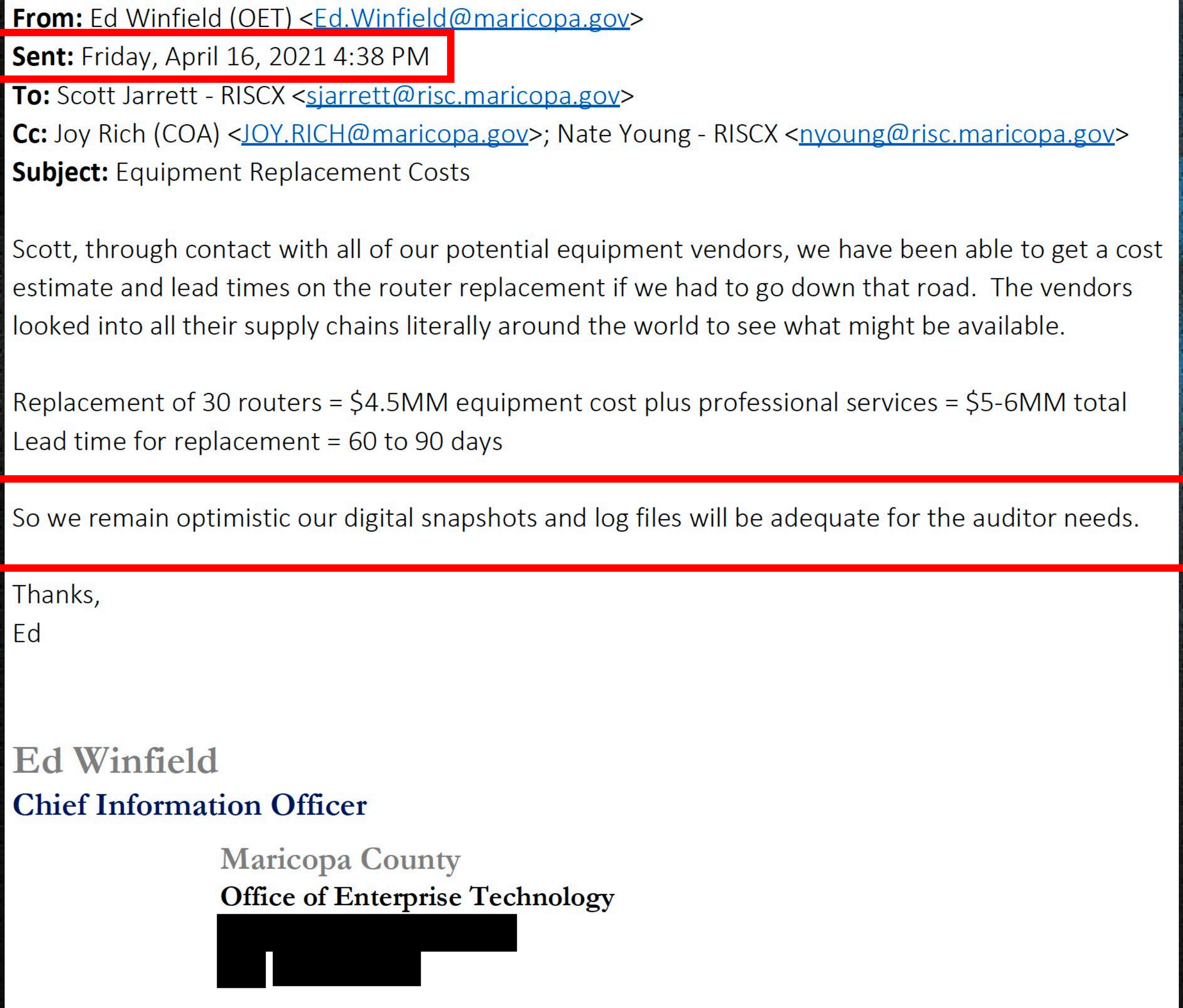
Telnet Connection. 74



```
The IP address is defined on the default VLAN (VLAN #1), of which all
ports are members. This is the IP address you use to access the CLI,
Web interface, or SNMP interface for the switch.To setup an IP
address:

Please enter the IP address of the device (A.B.C.D):[1.1.1.1]
```

Arizona Senate Audit

They Had the Network Logs in April 2021



From: Ed Winfield (OET) <Ed.Winfield@maricopa.gov>
Sent: Friday, April 16, 2021 4:38 PM
To: Scott Jarrett - RISCX <sjarrett@risc.maricopa.gov>
Cc: Joy Rich (COA) <JOY.RICH@maricopa.gov>; Nate Young - RISCX <nyoung@risc.maricopa.gov>
Subject: Equipment Replacement Costs

Scott, through contact with all of our potential equipment vendors, we have been able to get a cost estimate and lead times on the router replacement if we had to go down that road. The vendors looked into all their supply chains literally around the world to see what might be available.

Replacement of 30 routers = $4.5MM equipment cost plus professional services = $5-6MM total
Lead time for replacement = 60 to 90 days

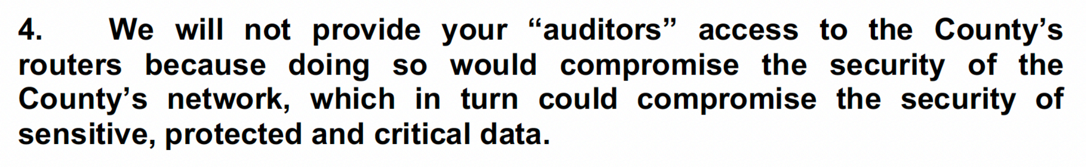
So we remain optimistic our digital snapshots and log files will be adequate for the auditor needs.

Thanks,
Ed

Ed Winfield
Chief Information Officer

Maricopa County
Office of Enterprise Technology
[redacted]

2021.05.17 Response Letter to Senate President Fann - FINAL_202105171430291332.pdf



4. We will not provide your "auditors" access to the County's routers because doing so would compromise the security of the County's network, which in turn could compromise the security of sensitive, protected and critical data.

Arizona Senate Audit

Questions?

EXHIBIT B

STATE OF MICHIGAN

IN THE CIRCUIT COURT FOR THE COUNTY OF ANTRIM

WILLIAM BAILEY	
Plaintiff	Case No. 20-9238-CZ
v.	
ANTRIM COUNTY	HON. KEVIN A. ELSENHEIMER
Defendant,	
SECRETARY OF STATE JOCELYN BENSON	
Intervenor-Defendant,	

Matthew S. DePerno (P52622)
DEPERNO LAW OFFICE, PLLC
Attorney for Plaintiff
951 W. Milham Avenue
PO Box 1595
Portage, MI 49081
(269) 321-5064

Haider A. Kazim (P66146)
CUMMINGS, MCCLOREY, DAVIS & ACHO, PLC
Attorney for Defendant
319 West Front Street
Suite 221
Traverse City, MI 49684
(231) 922-1888

Heather S. Meingast (P55439)
Erik A. Grill (P64713)
Assistant Attorneys General
Attorneys for Proposed Intervenor-Defendant Benson
PO Box 30736
Lansing, MI 48909
(517) 335-7659

AFFIDAVIT OF BENJAMIN R. COTTON 8 APRIL 2021

I, Ben Cotton, being duly sworn, hereby depose and state as follows:

1) I am over the age of 18, and I understand and believe in the obligations of an oath. I make this affidavit of my own free will and based on first-hand information and my own personal observations.

2) I am the founder of CyFIR, LLC (CyFIR).

3) I have a master's degree in Information Technology Management from the University of Maryland University College. I have numerous technical certifications, including the Certified Information Systems Security Professional (CISSP), Microsoft Certified Professional (MCP), Network+, and Certified CyFIR Forensics and Incident Response Examiner.

4) I have over twenty five (25) years of experience performing computer forensics and other digital systems analysis.

5) I have over eighteen (18) years of experience as an instructor of computer forensics and incident response. This experience includes thirteen (13) years of experience teaching students on the Guidance Software (now OpenText) EnCase Investigator and EnCase Enterprise software.

6) I have testified as an expert witness in state and federal courts and before the United States Congress.

7) I regularly lead engagements involving digital forensics for law firms, corporations, and government agencies.

8) In connection with this legal action I have had the opportunity to examine the following devices:

a) Antrim County Election Management Server Image. This image was acquired on 4 December 2020 by a firm named Sullivan and Strickler.

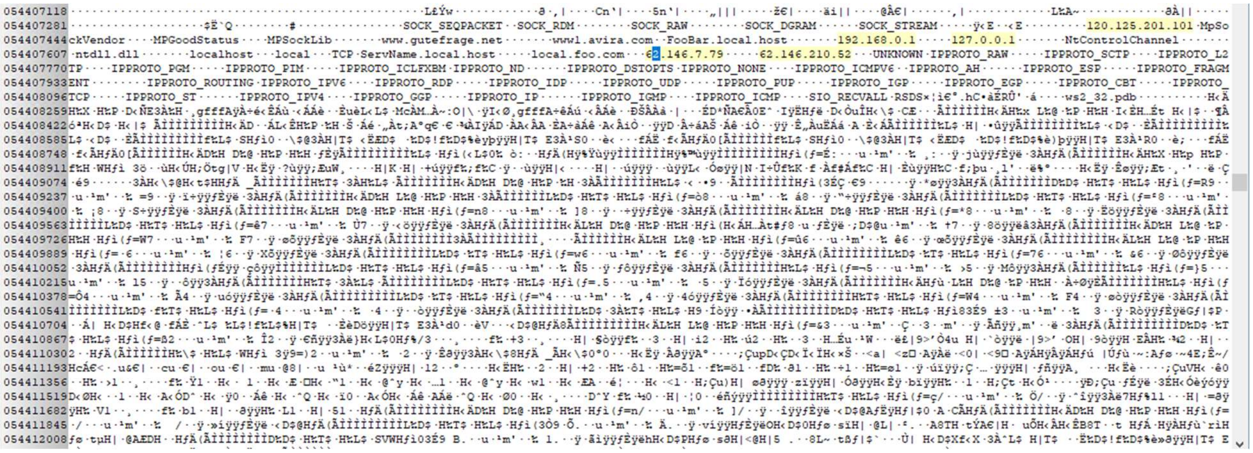
b) Thirty eight (38) forensic images of the compact flash cards used in Antrim County during the November 2020 elections that were imaged on 4 December 2020 by a firm named Sullivan and Strickler.

c) One (1) SID-15v-Z37-A1R, commonly known as the Image Cast X (ICX), that was used in the November 2020 elections

d) Two (2) Thumbdrives that were configured for a precinct using the ES&S DS400 tabulator that were used during the November 2020 election.

e) One ES&S server that was used in the November 2020 election.

9) **Internet Communications with the Dominion ICX.** I examined the forensic image of a Dominion ICX system utilized in the November 2020 election and discovered evidence of internet communications to a number of public and private IP addresses. Of specific concern was the presence of the IP address 120.125.201.101 in the unallocated space of the 10th partition of the device. This IP address resolves back to the Ministry of Education Computer Center, 12F, No 106, Sec.2,Hoping E. Rd.,Taipei Taiwan 106. This IP address is contextually in close proximity to data that would indicate that it was part of the socket configuration and stream of an TCP/IP communication session. Located at physical sector 958273, cluster 106264, sector offset 256, file offset 54407424 of the storage drive, the unallocated nature of the artifact precludes the exact definition of the date and time that this data was created. Also located in close proximity to the Ministry of Education IP address is the IP address 62.146.7.79. This IP address resolves to a cloud provider in Germany.



```
054407118 ··············································L£Ýw···········ə·,|····Cn'|····5n'|····„|||·····ž€|····äi||····@Â€|······,|············L‰A~·············əÀ||·····
054407281 ··················$Ë`Q·········#···············SOCK_SEQPACKET··SOCK_RDM········SOCK_RAW········SOCK_DGRAM······SOCK_STREAM·····ÿ‹E··‹E·········120.125.201.101·MpSo
054407444 ckVendor····MPGoodStatus····MPSockLib·······www.gutefrage.net·······www1.avira.com··FooBar.local.host·······192.168.0.1·····127.0.0.1·······NtControlChannel········
054407607 ·ntdll.dll·······localhost···local···TCP·ServName.local.host·····local.foo.com···62.146.7.79·····62.146.210.52···UNKNOWN·IPPROTO_RAW·····IPPROTO_SCTP····IPPROTO_L2
054407770 TP····IPPROTO_PGM·····IPPROTO_PIM·····IPPROTO_ICLFXBM·IPPROTO_ND······IPPROTO_DSTOPTS·IPPROTO_NONE····IPPROTO_ICMPV6··IPPROTO_AH······IPPROTO_ESP·····IPPROTO_FRAGM
054407933 ENT·········IPPROTO_ROUTING·IPPROTO_IPV6····IPPROTO_RDP·····IPPROTO_IDP·····IPPROTO_UDP·····IPPROTO_PUP·····IPPROTO_IGP·····IPPROTO_EGP·····IPPROTO_CBT·····IPPROTO_
054408096 TCP·····IPPROTO_ST······IPPROTO_IPV4····IPPROTO_GGP·····IPPROTO_IP······IPPROTO_IGMP····IPPROTO_ICMP····SIO_RECVALL·RSDS×¦i€°.hC•àÉRÛ'·á····ws2_32.pdb··········H‹Ä
```

Figure 1-IP Addresses Located in Unallocated Space

Further examination of the ICX clearly indicates that this system is also actively configured to communicate on a private network of 10.114.192.x with FTP settings to connect to 10.114.192.12 and 10.114.192.25. Also apparent is that at one time this system was configured to have the IP address 192.168.1.50. This IP address is also a private IP range. These IP configurations and artifacts definitively identify two things, 1) the device has been actively used for network communications and 2) that this device has communicated to public IP addresses not located in the United States. Further analysis and additional devices would be required to determine the timeframe of these public IP communications.

10) **<u>ESS DS400 Communications. </u>** A careful examination of the ESS DS400 devices and thumb drives was conducted. This examination proved that each DS400 had a Verizon cellular wireless communications card installed and that the card was active on powerup, which meant that there is the ability to connect to the public internet on these devices as well. Both of the DS400 devices were configured to transmit election results to IP address 10.48.51.1. This is a private network, which means that it would only be accessible by the remote DS400 systems through leveraging the public internet and establishing a link to a communications gateway using a public IP or via a virtual private network (VPN). It is important to understand that this

communication can only occur if the cellular modems have access to the public internet. I did not have the entire communications infrastructure for the private network and given this lack of device production associated with the DS200, I can not say which other devices may have connected to this private network nor the full extent of the communications of nor the remote accesses to the DS400 devices.

11) **Out of Date Security Updates and Virus Definitions.** An analysis of operating system, and antivirus settings on the servers and computers provided to me was conducted. It was immediately apparent that these systems were extremely vulnerable to unauthorized remote access and manipulation. For example, none of the operating systems had been patched nor the antivirus definition files updated for years. The Antrim EMS was last updated in 2016. The other systems were in a similar state. This lack of security updating has left these systems in an extremely vulnerable state to remote manipulation and hacking. Since 2016 more than ninety seven (97) critical updates have been issued for the Windows 10 operating system to prevent unauthorized access and hacking. The fact that these systems are in such a state of vulnerability, coupled with the obvious public and private internet access, calls the integrity of the voting systems into question. The Halderman report dated March 26, 2021 relating to this matter validates this finding. It also validates that the system is in a state such that an unauthorized user can easily bypass the passwords for the system and database to achieve unfettered access to the voting system in a matter of minutes. These manipulations and password bypass methodologies can be performed remotely if the unauthorized user gains access to the system through the private network or the public internet.

12) **Incomplete Compliance with the Subpoena for Digital Discovery.** Antrim County has apparently failed to produce all of the voting equipment for digital preservation and analysis. I

examined the purchase documents produced by Antrim County with respect to the purchase of the Dominion Voting system and note that the following system components listed on the purchase documents were not produced:

(a) ImageCast Listener Express Server

(b) ImageCast Express Firewall

(c) EMS Express Managed Switch

(d) ICP Wireless Modems (17)

(e) Image Cast Communications Manager Server

(f) ImageCast Listener Express RAS (remote access server) System

(g) ImageCast USB Modems (5)

Without these system components it will be impossible to determine the extent of public and private communications, the extent to which remote access to the voting system components is possible and to determine if or when unauthorized access occurred.

SIGNED UNDER THE PAINS AND PENALTIES OF PERJURY THIS 8th DAY OF April 2021.

Benjamin R. Cotton

EXHIBIT C

Maricopa County
Board of Supervisors

301 West Jefferson Street
10th Floor
Phoenix, AZ 85003-2143
Phone: 602-506-3406
www.maricopa.gov

May 17, 2021

VIA EMAIL ONLY

The Honorable Karen Fann
President of the Arizona Senate
Fifty-Fifth Legislature
1700 West Washington
Senate Building
Phoenix, Arizona, 85007
kfann@azleg.gov

Re: Response to your May 12, 2021 letter to Chairman Sellers

Senate President Fann,

We write in response to your May 12, 2021 letter. We also write in response to the May 12th social media post from the Twitter account, run by you or your designee/s, which accused Maricopa County of "deleting a directory full of databases from the 2020 election cycle days before the election equipment was delivered to the audit," and went on to accuse the County of "spoliation of evidence."

These accusations are false, defamatory, and beneath the dignity of the Senate. They are an insult to the dedicated public servants in the Maricopa County Elections Department and Office of the Recorder, who work incredibly long hours conducting the County's elections with integrity and honor.

1. Your accusation, that Maricopa County deleted data, is false.

You claim "the entire 'Database' directory from the D drive of the machine EMSPrimary has been deleted." This is false: the "Database" was not deleted from the server. And an analysis of the screenshot you provided (the "screenshot"), which we reproduce below, further proves that fact.

We demand that you immediately rescind your false and malicious tweet asserting that Maricopa County "spoiled evidence" in the days before we provided the server to the Senate. Your tweet, which relies on the "modified date" shown in the screenshot as evidence of wrongdoing, is demonstrably false; the only thing it does demonstrate is your auditors' incompetence. Their stunning lack of a basic understanding for how their software works is egregious and only made worse by the false tweet sent defaming the hardworking employees of Maricopa County.

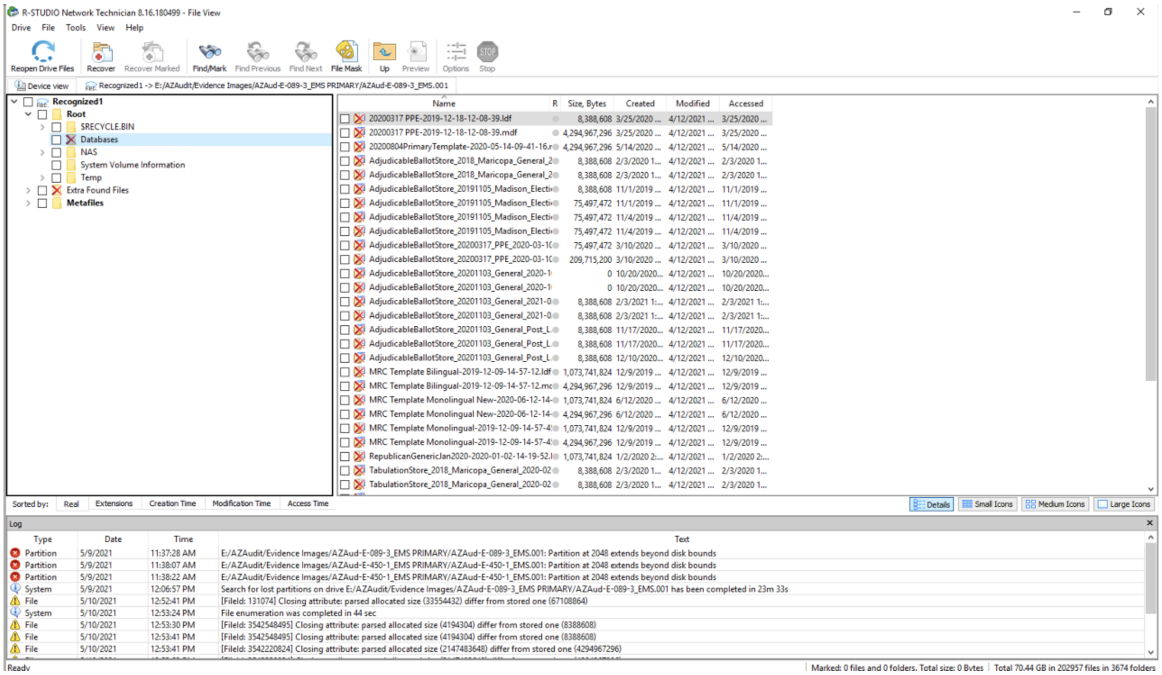
That the Senate would launch such a grave accusation via Twitter not only before waiting for an answer to your questions, but also *before* your so called "audit" demonstrates to the world that the Arizona Senate is not acting in good faith, has no intention of learning anything about the November 2020 General Election, but is only interested in feeding the various festering conspiracy theories that fuel the fundraising schemes of those pulling your strings. You have rented out the once good name of the Arizona State Senate to grifters and con-artists, who are fundraising hard-earned money from our fellow citizens even as your contractors parade around the Coliseum, hunting for bamboo and something they call "kinematic artifacts" while shining purple lights for effect. None of these things are done in a serious audit. The result is that the Arizona Senate is held up to ridicule in every corner of the globe and our democracy is imperiled.

On April 12, 2021, the Elections Department shut down the server to be packed up and made ready for delivery to the Senate. At no point was any data deleted when shutting down the server and packing up the equipment. Windows Servers will often change the "metadata" (additional data on files such as creation date, access date, modified date, owner, etc.) on Microsoft SQL database files based on actions performed on the Microsoft SQL (MSQL) Services that are needed to run the databases. The modified dates on the files are identical in the screen shots because that is when the server was shut down, and the (MSQL) services themselves were shut down, causing the server to update the metadata on all the files to the specific time when the services were shut down. Nothing was "deleted" on April 12, 2021.

Maricopa County provided you the actual Dominion server as commanded by your subpoena and we did not transfer or delete from that server *any* data from the 2020 General Election that was subject to your subpoena. You have now returned that server to us. Evidently your "auditors" made a copy of that server and are conducting their analysis on the copy.

The screenshot reveals that your "auditors" were using R-Studio Network Technician to conduct their analysis. That software is used to identify files that are *missing* at the spot the software is told to search. Yet you provided the screenshot falsely asserting that these identified "missing files" were deleted and evidence was "spoiled". Nothing in this screenshot indicates that any file was deleted or spoiled. At most what can be discerned from this screenshot is that R-Studio, as used by your "auditors," did not locate within the copy your vendor created the particular files listed in the column on the right.

Still, these files, and the Database, have the ominous red X-mark. We cannot say for certain what that mark indicates—other than that it likely indicates that R-Studio was unable to locate the files. The screenshot does not identify what type of search your "auditors" ran, and you conveniently failed to provide the full report the search generated. However, the table at the bottom of the screenshot appears to indicate that certain data is missing because it "extends beyond disk bounds" of the copied hard drive searched. Perhaps these files have the red X-mark because your "auditors" copied them to a segment of the hard drive that, in lay terms, is unreadable by the R-Studio software. Or because your "auditors" set the R-Studio search parameters incorrectly, such that it searched for these files in an area of the hard drive where they do not reside. There could be other explanations as well, including the possibility that your "auditors" inadvertently, or purposefully, moved—or even deleted—certain data.



Name	R	Size, Bytes	Created	Modified	Accessed
☐ 20200317 PPE-2019-12-18-12-08-39.ldf	●	8,388,608	3/25/2020 ...	4/12/2021 ...	3/25/2020 ...
☐ 20200317 PPE-2019-12-18-12-08-39.mdf	●	4,294,967,296	3/25/2020 ...	4/12/2021 ...	3/25/2020 ...
☐ 20200804PrimaryTemplate-2020-05-14-09-41-16.r	●	4,294,967,296	5/14/2020 ...	4/12/2021 ...	5/14/2020 ...
☐ AdjudicableBallotStore_2018_Maricopa_General_2	●	8,388,608	2/3/2020 1...	4/12/2021 ...	2/3/2020 1...
☐ AdjudicableBallotStore_2018_Maricopa_General_2	●	8,388,608	2/3/2020 1...	4/12/2021 ...	2/3/2020 1...
☐ AdjudicableBallotStore_20191105_Madison_Electi	●	8,388,608	11/1/2019 ...	4/12/2021 ...	11/1/2019 ...
☐ AdjudicableBallotStore_20191105_Madison_Electi	●	75,497,472	11/1/2019 ...	4/12/2021 ...	11/1/2019 ...
☐ AdjudicableBallotStore_20191105_Madison_Electi	●	75,497,472	11/4/2019 ...	4/12/2021 ...	11/4/2019 ...
☐ AdjudicableBallotStore_20191105_Madison_Electi	●	75,497,472	11/4/2019 ...	4/12/2021 ...	11/4/2019 ...
☐ AdjudicableBallotStore_20200317_PPE_2020-03-1(	●	75,497,472	3/10/2020 ...	4/12/2021 ...	3/10/2020 ...
☐ AdjudicableBallotStore_20200317_PPE_2020-03-1(	●	209,715,200	3/10/2020 ...	4/12/2021 ...	3/10/2020 ...
☐ AdjudicableBallotStore_20201103_General_2020-1		0	10/20/2020...	4/12/2021 ...	10/20/2020...
☐ AdjudicableBallotStore_20201103_General_2020-1		0	10/20/2020...	4/12/2021 ...	10/20/2020...
☐ AdjudicableBallotStore_20201103_General_2021-0.	●	8,388,608	2/3/2021 1:...	4/12/2021 ...	2/3/2021 1:...
☐ AdjudicableBallotStore_20201103_General_2021-0.	●	8,388,608	2/3/2021 1:...	4/12/2021 ...	2/3/2021 1:...
☐ AdjudicableBallotStore_20201103_General_Post_L.	●	8,388,608	11/17/2020...	4/12/2021 ...	11/17/2020...
☐ AdjudicableBallotStore_20201103_General_Post_L.	●	8,388,608	11/17/2020...	4/12/2021 ...	11/17/2020...
☐ AdjudicableBallotStore_20201103_General_Post_L.	●	8,388,608	12/10/2020...	4/12/2021 ...	12/10/2020...
☐ MRC Template Bilingual-2019-12-09-14-57-12.ldf	●	1,073,741,824	12/9/2019 ...	4/12/2021 ...	12/9/2019 ...
☐ MRC Template Bilingual-2019-12-09-14-57-12.mc	●	4,294,967,296	12/9/2019 ...	4/12/2021 ...	12/9/2019 ...
☐ MRC Template Monolingual New-2020-06-12-14-	●	1,073,741,824	6/12/2020 ...	4/12/2021 ...	6/12/2020 ...
☐ MRC Template Monolingual New-2020-06-12-14-	●	4,294,967,296	6/12/2020 ...	4/12/2021 ...	6/12/2020 ...
☐ MRC Template Monolingual-2019-12-09-14-57-4	●	1,073,741,824	12/9/2019 ...	4/12/2021 ...	12/9/2019 ...
☐ MRC Template Monolingual-2019-12-09-14-57-4	●	4,294,967,296	12/9/2019 ...	4/12/2021 ...	12/9/2019 ...
☐ RepublicanGenericJan2020-2020-01-02-14-19-52.l	●	1,073,741,824	1/2/2020 2:...	4/12/2021 ...	1/2/2020 2:...
☐ TabulationStore_2018_Maricopa_General_2020-02	●	8,388,608	2/3/2020 1...	4/12/2021 ...	2/3/2020 1...
☐ TabulationStore_2018_Maricopa_General_2020-02	●	8,388,608	2/3/2020 1...	4/12/2021 ...	2/3/2020 1...

```
Type       Date       Time         Text
Partition  5/9/2021   11:37:28 AM  E:/AZAudit/Evidence Images/AZAud-E-089-3_EMS PRIMARY/AZAud-E-089-3_EMS.001: Partition at 2048 extends beyond disk bounds
Partition  5/9/2021   11:38:07 AM  E:/AZAudit/Evidence Images/AZAud-E-450-1_EMS PRIMARY/AZAud-E-450-1_EMS.001: Partition at 2048 extends beyond disk bounds
Partition  5/9/2021   11:38:22 AM  E:/AZAudit/Evidence Images/AZAud-E-450-1_EMS PRIMARY/AZAud-E-450-1_EMS.001: Partition at 2048 extends beyond disk bounds
System     5/9/2021   12:06:57 PM  Search for lost partitions on drive E:/AZAudit/Evidence Images/AZAud-E-089-3_EMS PRIMARY/AZAud-E-089-3_EMS.001 has been completed in 23m 33s
File       5/10/2021  12:52:41 PM  [FileId: 131074] Closing attribute: parsed allocated size (33554432) differ from stored one (67108864)
System     5/10/2021  12:53:24 PM  File enumeration was completed in 44 sec
File       5/10/2021  12:53:30 PM  [FileId: 3542548495] Closing attribute: parsed allocated size (4194304) differ from stored one (8388608)
File       5/10/2021  12:53:41 PM  [FileId: 3542548495] Closing attribute: parsed allocated size (4194304) differ from stored one (8388608)
File       5/10/2021  12:53:41 PM  [FileId: 3542220824] Closing attribute: parsed allocated size (2147483648) differ from stored one (4294967296)
```

```
Ready    Marked: 0 files and 0 folders. Total size: 0 Bytes    Total 70.44 GB in 202957 files in 3674 folders
```

Regardless, the failure of your so called "auditors" to locate data files on the copy *they* made of the County's server speaks more to their ineptitude than it does to the integrity and actions of our dedicated public employees who effectively and accurately run the elections in the fourth largest county in the United States.

2. Your various questions about our election procedures reveal a serious lack of understanding of election law, as well as the best

practices utilized by Maricopa County and other jurisdictions for the conduct of elections.

In your letter, you asked a number of questions. We will answer each in turn.

Your First Question: The County has not provided any chain-of-custody documentation for the ballots. Does such documentation exist, and if so, will it be produced?

The Answer:

We are stunned that you are asking us this question. It demonstrates a spectacular lack of understanding on your part of what occurred during the County's transfer of its material to your custody. Simply stated, your liaison, Ken Bennett, was provided with the documentation demonstrating chain of custody. And your counsel, Mr. Langhofer, was consulted as to the final form of that chain of custody documentation. To summarize:

- The Elections Department transported the subpoenaed material from the Maricopa County Tabulation and Election Center (MCTEC) to your custody at the Arizona Veterans Memorial Coliseum in box trucks secured with a tamper-evident seal after being loaded at MCTEC.
- MCSO deputies observed the trucks being loaded and then escorted the trucks to the Coliseum.
- Mr. Bennett gave approval to unload each truck. All the tamper-evident seals were photographed by the Senate's contractors as well as by County representatives to confirm that the seals were still intact. And, Mr. Bennett or his designee personally observed each seal being broken before the trucks were unloaded.
- Each truck had a detailed manifest prepared by the Elections Department listing with specificity every item on the truck, including serial numbers for all of the equipment, and the identifying information for each box of ballots.
- Mr. Bennett and Co-Elections Director Scott Jarrett together reviewed the delivery, comparing each item that had been delivered to the manifest for that truck.
- Each confirmed, together, that the items identified on the manifest were delivered by the County to the Senate.
- Each signed the manifest, attesting to its accuracy. After that point in time, County personnel no longer touched the material that had been

transferred to the Senate's custody, and the Senate's contractors moved the material to the areas of the Coliseum in which they determined to store it.

- Once delivery was complete, counsel for the County prepared a document evidencing the chain of custody of the materials delivered, with the manifests as an exhibit stating that the items in the manifests had been delivered from the County to the Senate's custody.
- Alexander Kolodin, then counsel for the Senate's contractor, Cyber Ninjas, sent a copy of the document to your attorney, Kory Langhofer, so he could provide any input.
- Mr. Jarrett signed the letter on April 29, 2021, attesting that the delivered materials had been in the County's custody and control at all times from the November 3, 2020 election until it was delivered to the Senate.
- Mr. Bennett subsequently signed the letter and he has a fully executed copy of it.

In short, both the Senate and the County have been given sufficient chain of custody documentation for the ballots, which currently remain in your custody. Your suggestion to the contrary is demonstrably wrong.

Your Second Question: The bags in which the ballots were stored are not sealed, although the audit team has found at the bottom of many boxes cut seals of the type that would have sealed a ballot bag. Why were these seals placed at the bottom of the boxes?

The Answer:

The bags in which Election Day ballots were stored *were* sealed, and the seals you found in the bottom of boxes containing Election Day ballots came off these bags. Pursuant to law (A.R.S §16-608 and Chapter 9 of Elections Procedures Manual), all Election Day ballots are transported by bi-partisan teams from vote centers to MCTEC in tamper evident sealed black canvas bags. After the Statewide Canvass and the subsequent five-day contest period concludes, teams of bi-partisan employees transfer the contents of the black canvas bags, along with the tamper evident seals that were affixed on the bag, to the long-term ballot storage boxes. Below are examples of the canvas bags and seals (they made be red, green or blue) used during transport and short-term storage.

Your Third Question: Batches within a box are frequently separated by only a divider without any indication of the corresponding batch numbers. In some cases, the batch dividers are missing altogether. This lack of organization has significantly complicated and delayed the audit team's ballot processing efforts. What are the County's procedures for sorting, organizing, and packaging ballot batches?

The Answer:

It is the Elections Department's practice to divide batches of ballots using the Early Voting Transmittal Slips. But no law requires the Elections Department to do that—it is something that its staff try to do as a best practice. It is possible that a slip log fell out from between the ballots during transport to the Coliseum, or due to handling by your contractors—we cannot say. Regardless, the slip logs should still be in the boxes.

It is obvious your "audit" of the ballots is moving at a slower pace than you planned. Our organization of the ballots in the boxes—an organization that complies with the laws that the Senate helped write—is no excuse for why you are some 1.5 million ballots behind schedule in your "recount", as your letter comically insinuates.

Your Fourth Question: Most of the ballot boxes were sealed merely with regular tape and not secured by any kind of tamper-evident seal. Is that the County's customary practice for storing ballots?

The Answer:

Yes, that is the County's customary practice. As required by law (A.R.S. § 16-624 and Chapter 13, Part VI of the Elections Procedures Manual at 248), the Elections Department seals each box of ballots for long-term storage with the County Treasurer. For Election Day ballots, we use tamper evident tape. As described above, Election Day ballots are temporarily stored in black canvas bags. Transferring the Election Day ballots from the canvas bag to a long-term storage box requires transport from a secure storage cage to the ballot tabulation center and vault. Even though the ballot storage cage and vault are only a short distance of less than 100 feet, we add the security precaution of tamper evident tape to ensure that the boxes are not tampered with during transport. Ballots tabulated at central count are immediately placed in long-term ballot storage boxes and moved to our secure ballot vault.

The vault is one of the most secure areas within the Elections Department and has highly restricted access among numerous overhead security cameras. The boxes are sealed with standard clear sturdy packing tape. While in the custody of the Elections Department and with the exception of the batches of ballots used for the Hand Count, these ballots never leave the custody of the ballot tabulation center and secure ballot vault.

Finally, the long-term storage boxes that include batches of early ballots selected by the political parties and included in the hand count are affixed with tamper evident tape. This extra security measure is provided because these batches of ballots are removed from the vault to be hand counted by the political parties. The hand count boards confirm the tamper evident tape has not been modified prior to beginning the hand count procedures.

Your Fifth Question: The audit team has encountered a significant number of instances in which there is a disparity between the actual number of ballots contained in a batch and the total denoted on the pink report slip accompanying the batch. In most of these instances, the total on the pink report slip is greater than the number of ballots in the batch, although there are a few instances in which the total is lower. What are the reasons for these discrepancies? For your reference, please see several illustrative (*i.e.*, not comprehensive) examples in the table below:

Pallet	Ballot Type	Batch	Pink Slip Total	Actual Total	Discrepancy
5	EV	2104	200	198	-2
5	EV	9276	200	165	-35
15	EV	9278	200	187	-13
15	EV	1643	200	218	18
7	EV	6359	197	187	-10

The Answer:

The slip logs you are referencing are called “Early Voting Transmittal Slips.” Because it is obvious that your contractors have no understanding of these matters, a brief tutorial is in order:

Early ballots returned by voters to MCTEC are placed into batches of approximately 200 ballots and then examined by bipartisan Early Ballot Processing Boards ("EV Processing Boards"). The EV Processing Boards check the ballots in each batch with the human eye to determine whether, in their judgment, the ballots are capable of being tabulated by the tabulation machines, or whether they are damaged such that they will not be read by the machines but must be duplicated pursuant to statute (A.R.S. § 16-621(A)). Examples of damaged ballots that cannot be read by the tabulators include ballots that are ripped or those that have had a drink spilled on them. Because it is obvious the tabulators will not read such damaged ballots, those ballots are removed from the batch and sent to a bipartisan Ballot Duplication Board to be duplicated onto a new ballot as required by statute. (A.R.S. § 16-621(A) and Elections Procedures Manual, Chapter 10, Part II(D) at 201). All such duplicated ballots are then tabulated by the tabulation equipment, as the law requires. The rest of the ballots in the batch are sent to the Central Count Tabulators to be tabulated.

The Early Voting Transmittal Slips that you referenced in your letter are prepared by the EV Processing Boards to track how many ballots from each batch of approximately 200 are sent to the Central Count Tabulators. These Transmittal Slips exist as a three-part carbon copy form. After the EV Processing Board completes the form, the three copies are separated. One copy accompanies the ballots to the tabulation center, so that the elections officials who insert the ballots into the Central Count Tabulators can verify that they have received the correct number of ballots for tabulation. The other two copies of the Transmittal Slip are used for other tracking purposes.

But not every ballot that is sent for tabulation can be read by the tabulators. Sometimes the voters make stray marks that interfere with the tabulation process. Or, the early ballot is printed slightly off-center. These unreadable ballots are rejected when inserted into the Central Count Tabulators. In these instances, those damaged ballots are sent to the bipartisan Ballot Duplication Boards directly from the central count tabulation center.

To maintain the integrity of the data on all copies of the now-separated, three-part Early Voting Transmittal Slip, the Elections Department uses a *separate* set of tabulator logs to track when a damaged ballot is sent to duplication from the central count tabulation center. To the point: the ballots that are sent directly to duplication from the tabulation center are not tracked on the slip logs you referenced in your letter, rather they are tracked on Daily Tabulator Log slips, prepared contemporaneously when the ballots are tabulated.

For example, consider the first slip log you referenced, referring to Batch

2104. We reproduce it here:

Pallet	Ballot Type	Batch	Pink Slip Total	Actual Total	Discrepancy
5	EV	2104	200	198	-2

This Transmittal Slip records that the EV Processing Board sent all 200 ballots in Batch 2104 to the central count tabulation center. However, when the ballots were inserted into the tabulation equipment, two of the ballots could not be read. Thus, when you examined this batch of ballots, only 198 ballots were included, which is why you erroneously believed there was a discrepancy of 2 ballots. Your contractors misunderstand the purpose of the Transmittal Slip records. That record indicates the number of ballots from Batch 2104 that were transferred by the EV Processing Board directly to the central count tabulation center. In this instance, the Central Count Tabulators were unable to read two of those ballots in the batch of 200. Those two had to be sent from the tabulation center to the bipartisan Duplication Boards. Thus, only 198 ballots in Batch 2104 were immediately tabulated by the Central Count Tabulators, which is why you only found 198 ballots from Batch 2104 in the cardboard box. (The duplicated ballots are kept in other sealed boxes after they are tabulated).

Our examination of the corresponding Daily Tabulator Log slips for batch 2104 confirms this. The Daily Tabulator Log slips reveal how many ballots from each batch received by the tabulation personnel are tabulated by the equipment, and how many ballots from each batch that arrive at the tabulation center have to be sent to be duplicated in order to be tabulated. The Daily Tabulator Log slip that includes Batch 2104 reveals that 2 ballots of the 200-ballot batch were rejected by the tabulators and were sent to the bipartisan Duplication Boards.

We likewise determined that, based on the Daily Tabulator Log slips for Batches 9276, 9278, and 6359, the “discrepancies” you identified were not discrepancies, but rather accurately reflected damaged ballots being sent from the tabulation center to be duplicated because they could not be read by the tabulator.

Batch 1643 presents a different issue. We reproduce it here:

Pallet	Ballot Type	Batch	Pink Slip Total	Actual Total	Discrepancy

15	EV	1643	200	218	18

You seem to be stating that you counted 218 ballots in Batch 1643, but our Transfer Transmittal Slip log only recorded 200 ballots. We examined the Daily Tabulator Log slip for Batch 1643, and have verified that there were only 200 ballots in that batch—as there should have been. We also verified that the Daily Tabulator Log slip indicates that zero of the 200 ballots were sent from the tabulation center to be duplicated, but rather all 200 ballots were immediately able to be tabulated by the Central Count Tabulators. Thus, there should have been—and, we believe there were—200 ballots in Batch 1643 in the sealed box, not 218 as your contractors counted.

3. We cannot produce what we do not possess; and, we do not possess additional passwords.

In your letter, you state that Maricopa County "has refused to provide passwords necessary to access vote tabulation devices." However, as we have previously told you, we have produced every password in our custody and control. You, however, accuse us of lying. You state that we could not have conducted our forensic audits without additional passwords, and that "it strains credulity" to suggest that our contract with Dominion Voting Systems does not allow us to obtain additional, proprietary passwords belonging to Dominion.

The contract is a public record: you could have requested it. Even a cursory review would show there is no contractual provision granting the County the ability to acquire Dominion's proprietary passwords. Instead you call us liars and insult us, when a simple public records request would have helped you avoid such indecent conduct.

Next, let's consider the County's two separate forensic audits conducted in February of this year. You suggest that the Dominion proprietary password would have been necessary to conduct those audits. You are correct: it was. The forensic audit firms that the County hired, Pro V & V and SLI Compliance, are both accredited by the U.S. Elections Assistance Commission as voting system testing laboratories. Because of that accredited status, signifying that these firms are specialists who have expertise with voting systems and understand how to audit them, Dominion Voting Systems provides Pro V & V and SLI Compliance with the necessary passwords to audit their machines.

Your chosen "auditors," the Cyber Ninjas, are certainly many things. But "accredited by the EAC" is not one of them. Regardless, we cannot give you a password that we do not possess any more than we can give you the formula for Coca Cola. We do not have it; we have no legal right to acquire it; and so, we cannot give it to you.

4. We will not provide your "auditors" access to the County's routers because doing so would compromise the security of the County's network, which in turn could compromise the security of sensitive, protected and critical data.

The County's routers provide a blueprint to the County's network. Were that blueprint to fall into the wrong hands, the results could be catastrophic.

We can best explain it, in non-technical terminology, as follows: suppose your house had a hidden wall safe, where you stored your most valuable possessions. You would do everything possible to prevent criminals from finding the location of the safe. You wouldn't give anyone a blueprint of your house, with the location of the wall safe circled in red marker, because if criminals got ahold of it, they would know exactly where your valuables were. They could be in and out of your house and steal your most important possessions before law enforcement could arrive to stop them.

The County's routers are also a blueprint. They provide a map showing exactly where in the County's computer network all the County's most critical data is hidden—data related to the most sensitive law enforcement programs—including federal law enforcement programs, and data related to Maricopa County's citizens' protected health information, financial information, and social security numbers. If a criminal organization or some other bad actor gained access to that blueprint, it could do irreparable damage to the County, the State, and even our Country. That blueprint could allow someone who successfully hacked into our network to quickly copy all of this sensitive information—perhaps before we even knew that our security had been breached – because they would know exactly where to look. This could lead to any number of harms to our citizenry, including disruption to critical services or even identity theft. And, it could lead to the "outing" of undercover law enforcement personnel and the unraveling of critical law enforcement programs. Having this blueprint would also aid a bad actor trying to infect our network with ransomware that might lock us out of our network, further putting our citizens' protected information, and perhaps even their physical safety, at risk.

You have suggested, however, that we should let your contractors look at the routers anyway. Yet Mr. Bennett publicly acknowledged that your contractors locked him out of your "audit's" official twitter account, and also acknowledged that he was having difficulty regaining access. There is more we could say to explain why we do not believe it prudent to blindly trust your contractors, but we believe that example is enough. President Reagan famously said, "Trust, but verify." The requisite verification is not present here. Accordingly, we will not endanger the safety and security of our citizens, our law enforcement, our state, and our nation by providing you and your "auditors" access to our routers.

5. We will not attend your meeting on May 18, 2021.

In your letter, you invite us to attend a meeting at the Arizona State Capitol on Tuesday, May 18, 2021, at 1:00 p.m., and you request that we bring Election Department officials who would have knowledge of our elections procedures. We will not be attending. We will not be responding to any additional inquiries from your "auditors". Their failure to understand basic election processes is an indication you didn't get the best people to perform in your political theatre. We have wasted enough County resources. People's tax dollars are real, your "auditors" are not.

6. Your "audit" is harming all of us, and we ask you to end it.

Finally, we express our united view that your "audit", no matter what your intentions were in the beginning, has become a spectacle that is harming all of us. Our state has become a laughingstock. Worse, this "audit" is encouraging our citizens to distrust elections, which weakens our democratic republic.

Your "auditors" began the "audit" unaware that using blue pens on ballots could harm them, and apparently would have distributed blue pens to those conducting the recount of ballots had a reporter not informed them. It has gone downhill from there. Your "audit," which you once said was intended to increase voters' confidence in our electoral process, has devolved into a circus.

You are using purple lights and spinning tables. You are hunting for bamboo. These are not things that serious auditors of elections do.

You are photographing ballots contrary to the laws that the Senate helped enact, and you are sending those images to unidentified places and people. You have repeatedly lost control of your twitter account, which has tweeted things that appear to be the rantings of a petulant child—not the serious statements of a serious audit.

None of this is inspiring confidence. None of this will cause our citizens to trust elections. In fact, it is having the opposite result. You certainly must recognize that things are not going well at the Coliseum. You also must know that the County's election was free and fair, and that our Elections Department did an outstanding job conducting it.

Unfortunately, this has become a partisan issue, and it should not be one. It is time to make a choice to defend the Constitution and the Republic. As County elected officials, we come from different political parties, but we stand united together to defend the Constitution and the Republic in our opposition to the Big Lie. We ask everyone to join us in standing for the truth. The November 3, 2020 general election was free and fair and conducted by the Elections Department with integrity and honor.

Regardless of your intentions when you decided to subpoena our equipment and ballots, this cannot really be what you envisioned. You, Senate President Fann, are the only one with the power to immediately end it. We implore you to recognize the obvious truth: your "auditors" are in way over their heads. They do not have the experience necessary to conduct an audit of an election. They do not know the laws, nor the procedures, nor the best practices. It is inevitable that they will arrive at questionable conclusions.

It is time to end this. For the good of the Senate, for the good of the Country and for the good of the Democratic institutions that define us as Americans.

SIGNATURES ON FOLLOWING PAGE

Sincerely,

____
Jack Sellers, Chairman
Supervisor, District 1
Maricopa County Board of Supervisors

____
Stephen Richer
Maricopa County Recorder

____
Bill Gates, Vice Chairman
Supervisor, District 3
Maricopa County Board of Supervisors

____
Paul Penzone
Maricopa County Sheriff

____
Steve Chucri
Supervisor, District 2

____
Clint Hickman
Supervisor, District 4

____
Steve Gallardo
Supervisor, District 5

EXHIBIT D

United States Election Assistance Commission Report of Investigation

Dominion Voting Systems D-Suite 5.5-B

Williamson County, Tennessee

March 31, 2022

Jonathon Panek
Director, Voting System Testing and Certification

U.S. ELECTION ASSISTANCE COMMISSION
633 3rd St. NW, Suite 200
Washington, DC 20001

Contents

Introduction 2

Reported Anomaly 2

Formal Investigation 3

Testing and Analysis 3

Conclusion of Formal Investigation 4

Introduction

In late 2002, Congress passed the Help America Vote Act of 2002 (HAVA), which created the U.S. Election Assistance Commission (EAC) and vested it with the responsibility of setting voting system standards and providing for the testing and certification of voting systems. This mandate represented the first time the Federal government provided for the voluntary testing, certification, and decertification of voting systems nationwide. In response to this HAVA requirement, the EAC has developed the Federal Voting System Testing and Certification Program.

The EAC's Testing and Certification Program includes several quality monitoring tools that help ensure that voting systems continue to meet the EAC's voting system standards as the systems are manufactured, delivered, and used in Federal elections. These aspects of the program enable the EAC to independently monitor the continued compliance of fielded voting systems. One of these tools is field anomaly reporting.

Election officials may submit notices of voting system anomalies directly to the EAC. An anomaly is defined as an irregular or inconsistent action or response from the voting system, or system component, which resulted in the system or component not functioning as intended or expected. Anomaly reports may indicate a voting system is not in compliance with the Voluntary Voting System Guidelines or the procedural requirements of this EAC Testing and Certification Program.

An informal inquiry is the first step taken when information of this nature is presented to the EAC. The sole purpose of the informal inquiry is to determine whether a formal investigation is warranted. The outcome of an informal inquiry is limited to a decision on referral for investigation. A formal investigation is an official investigation by the EAC to determine whether a voting system warrants decertification. The result of a formal investigation is a Report of Investigation.

Reported Anomaly

On November 3, 2021, the EAC received a report from the Tennessee Secretary of State's (TN SoS) office that they were planning an investigation into an anomaly observed in Williamson County, Tennessee during a municipal election held on October 26, 2021, regarding Dominion D-Suite 5.5-B ImageCast Precinct (ICP) tabulators. Close poll reports from 7 of the 18 ICP tabulators used during the election did not match the number of ballots scanned. Subsequent tabulation on the jurisdiction's ICC central count scanner provided the correct tally. The central count tabulation was confirmed via hand count of the paper ballot records on October 27, 2021.

Discussions with the TN SoS on December 17, 2021, and January 5, 2022, following their investigation, provided additional details to the EAC. The details of the anomaly were confirmed and reproduced during the state investigation, though the root cause of the anomaly was not determined.

Formal Investigation

Based upon the information obtained from the TN SoS, the EAC initiated a formal investigation into the matter to determine the necessary actions to obtain the root cause and remedy the issue. The investigation was conducted at the Williamson County Elections Commission facility on January 19 through January 22, 2022. This analysis was performed by both EAC accredited Voting System Test Laboratories (VSTL), Pro V&V and SLI Compliance. The EAC, Williamson County staff, TN SoS, and Dominion staff were present during the analysis.

Testing and Analysis

The first step of the VSTL analysis was verification of the system configuration. Hashes of all components involved were collected and compared to the repository of hashes for the EAC certified system. It was discovered that the system was installed with outdated versions of two configuration files when the system was upgraded from D-Suite 5.5 to D-Suite 5.5-B in January of 2021.

Next, a copy of the election definition used on election day was used to make Compact Flash (CF) cards for the ImageCast Precinct (ICP) scanners and ImageCast X (ICX) ballot marking devices. This election definition was imported into the D-Suite 5.5-B system from a definition originally created on the D-Suite 5.5 system.

Ballots were printed from the ICX and tabulated through the ICP scanners. Multiple ICP scanners were used for tabulation including some that originally exhibited the anomaly during the election and some that did not. Following tabulation, close poll reports and audit logs from the ICP scanners were examined. Results showed that the anomaly was recreated on each of the ICP scanners. This process was repeated several times to understand and isolate the details of exactly when the anomaly occurred and circumstances that may have led to the anomaly occurring.

Analysis of audit log information revealed entries that coincided with the manifestation of the anomaly; a security error “QR code signature mismatch” and a warning message “Ballot format or id is unrecognizable” indicating a QR code misread occurred. When these events were logged, the ballot was rejected. Subsequent resetting of the ICP scanners and additional tabulation demonstrated that each instance of the anomaly coincided with the previously mentioned audit log entries, though not every instance of those audit log entries resulted in the anomaly.

Further analysis of the anomaly behavior showed that the scanners correctly tabulated all ballots until the anomaly was triggered. Following the anomaly, ballots successfully scanned and tabulated by the ICP were not reflected in the close poll reports on the affected ICP scanners.

Additional iterations of testing were performed after updating the configuration files previously mentioned to the proper versions associated with the D-Suite 5.5-B system. The anomaly was recreated using the correct configuration files with the originally programmed election definition.

A final test was performed using an election definition recreated entirely on the D-Suite 5.5-B system with identical parameters to the definition used during the election and for prior testing. The anomaly was not observed during this test, and there were no instances of the security error "QR code signature mismatch" or warning message "Ballot format or id is unrecognizable" in the audit log.

Conclusion of Formal Investigation

The direct cause of the anomaly was inconclusive. Based on the investigation, it's reasonable to conclude that the anomaly is related to the imported D-Suite 5.5 election definition used on the D-Suite 5.5-B system.

On February 11, 2022, Dominion submitted a Root Cause Analysis (RCA) to the EAC. The report indicates that erroneous code is present in the EAC certified D-Suite 5.5-B and D-Suite 5.5-C systems. The RCA report states that when the anomaly occurs, it's due to a misread of the QR code. If the QR code misread affects a certain part of the QR code, the ICP scanner mistakenly interprets a bit in the code that marks the ballot as provisional. Once that misread happens, the provisional flag is not properly reset after that ballot's voting session. The result is that every ballot scanned and tabulated by the machine after that misread is marked as provisional and thus, not included in the tabulator's close poll report totals.

Dominion has submitted Engineering Change Orders (ECO)s for the ICP software in the D-Suite 5.5-B and D-Suite 5.5-C systems: ECO 100826 and ECO 100827. Modified ICP source code was submitted by Dominion that resets the provisional flag following each voting session. The ECO analysis included source code review to confirm the change to both systems and to ensure no other code is changed. A Trusted Build of the modified source code was performed to produce the updated ICP software. This software was then tested for accuracy by processing two thousand ballots printed by an ICX, utilizing the same election definition used in Williamson County, TN on October 26, 2021.

The analysis and testing of the ECOs has demonstrated that the anomaly was successfully fixed. No instance of the anomaly or the associated error or warning messages in the ICP audit logs were observed during the testing. The EAC has approved ECO 100826 and ECO 100827 on March 31, 2022.

EXHIBIT E

STATE OF MICHIGAN

IN THE CIRCUIT COURT FOR THE COUNTY OF ANTRIM

WILLIAM BAILEY

Plaintiff

v.

ANTRIM COUNTY

Defendant,

SECRETARY OF STATE JOCELYN BENSON

Intervenor-Defendant,

Case No. 20-9238-CZ

HON. KEVIN A. ELSENHEIMER

Matthew S. DePerno (P52622)
DEPERNO LAW OFFICE, PLLC
Attorney for Plaintiff
951 W. Milham Avenue
PO Box 1595
Portage, MI 49081
(269) 321-5064

Haider A. Kazim (P66146)
CUMMINGS, MCCLOREY, DAVIS & ACHO, PLC
Attorney for Defendant
319 West Front Street
Suite 221
Traverse City, MI 49684
(231) 922-1888

Heather S. Meingast (P55439)
Erik A. Grill (P64713)
Assistant Attorneys General
Attorneys for Proposed Intervenor-Defendant Benson
PO Box 30736
Lansing, MI 48909
(517) 335-7659

AFFIDAVIT OF BENJAMIN R. COTTON 8 APRIL 2021

I, Ben Cotton, being duly sworn, hereby depose and state as follows:

1) I am over the age of 18, and I understand and believe in the obligations of an oath. I make this affidavit of my own free will and based on first-hand information and my own personal observations.

2) I am the founder of CyFIR, LLC (CyFIR).

3) I have a master's degree in Information Technology Management from the University of Maryland University College. I have numerous technical certifications, including the Certified Information Systems Security Professional (CISSP), Microsoft Certified Professional (MCP), Network+, and Certified CyFIR Forensics and Incident Response Examiner.

4) I have over twenty five (25) years of experience performing computer forensics and other digital systems analysis.

5) I have over eighteen (18) years of experience as an instructor of computer forensics and incident response. This experience includes thirteen (13) years of experience teaching students on the Guidance Software (now OpenText) EnCase Investigator and EnCase Enterprise software.

6) I have testified as an expert witness in state and federal courts and before the United States Congress.

7) I regularly lead engagements involving digital forensics for law firms, corporations, and government agencies.

8) In connection with this legal action I have had the opportunity to examine the following devices:

a) Antrim County Election Management Server Image. This image was acquired on 4 December 2020 by a firm named Sullivan and Strickler.

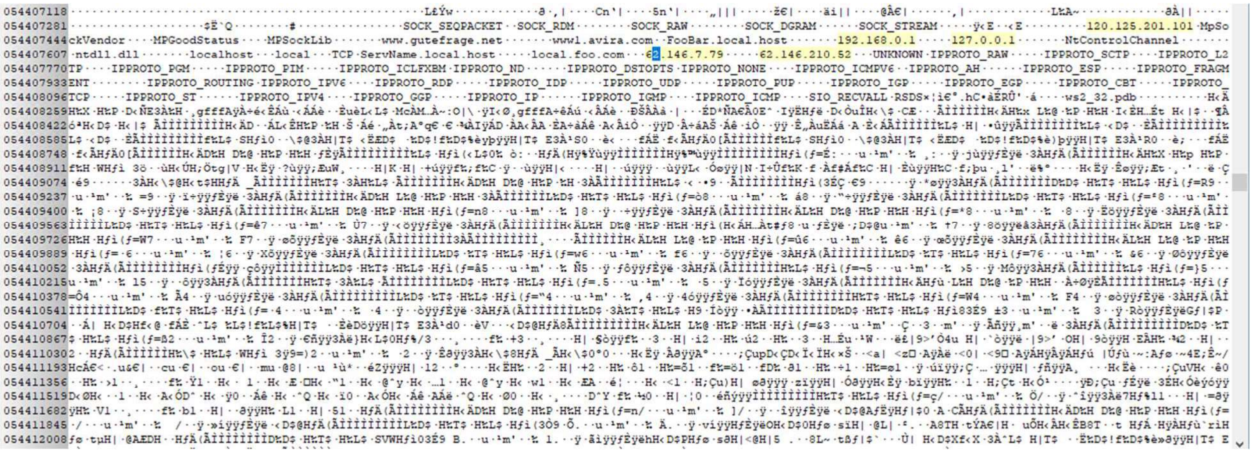
b) Thirty eight (38) forensic images of the compact flash cards used in Antrim County during the November 2020 elections that were imaged on 4 December 2020 by a firm named Sullivan and Strickler.

c) One (1) SID-15v-Z37-A1R, commonly known as the Image Cast X (ICX), that was used in the November 2020 elections

d) Two (2) Thumbdrives that were configured for a precinct using the ES&S DS400 tabulator that were used during the November 2020 election.

e) One ES&S server that was used in the November 2020 election.

9) **Internet Communications with the Dominion ICX.** I examined the forensic image of a Dominion ICX system utilized in the November 2020 election and discovered evidence of internet communications to a number of public and private IP addresses. Of specific concern was the presence of the IP address 120.125.201.101 in the unallocated space of the 10th partition of the device. This IP address resolves back to the Ministry of Education Computer Center, 12F, No 106, Sec.2,Hoping E. Rd.,Taipei Taiwan 106. This IP address is contextually in close proximity to data that would indicate that it was part of the socket configuration and stream of an TCP/IP communication session. Located at physical sector 958273, cluster 106264, sector offset 256, file offset 54407424 of the storage drive, the unallocated nature of the artifact precludes the exact definition of the date and time that this data was created. Also located in close proximity to the Ministry of Education IP address is the IP address 62.146.7.79. This IP address resolves to a cloud provider in Germany.



```
054407118 ····································L£Ýw···········ə·,|····Cn'|····5n'|····„|||·····ž€|····äi||····@Â€|······,|···········LžA~··············əÀ||·····
054407281 ···················$Ë`Q········#················SOCK_SEQPACKET··SOCK_RDM········SOCK_RAW········SOCK_DGRAM······SOCK_STREAM·····ÿ‹E··‹E·········120.125.201.101·MpSo
054407444ckVendor····MPGoodStatus····MPSockLib·······www.gutefrage.net·······www1.avira.com··FooBar.local.host·······192.168.0.1·····127.0.0.1·······NtControlChannel·······
054407607·ntdll.dll·······localhost···local···TCP·ServName.local.host·····local.foo.com···62.146.7.79·····62.146.210.52···UNKNOWN·IPPROTO_RAW·····IPPROTO_SCTP····IPPROTO_L2
054407770TP····IPPROTO_PGM·····IPPROTO_PIM·····IPPROTO_ICLFXBM·IPPROTO_ND······IPPROTO_DSTOPTS·IPPROTO_NONE····IPPROTO_ICMPV6··IPPROTO_AH······IPPROTO_ESP·····IPPROTO_FRAGM
054407933ENT········IPPROTO_ROUTING·IPPROTO_IPV6····IPPROTO_RDP·····IPPROTO_IDP·····IPPROTO_UDP·····IPPROTO_PUP·····IPPROTO_IGP·····IPPROTO_EGP·····IPPROTO_CBT·····IPPROTO_
054408096TCP·····IPPROTO_ST······IPPROTO_IPV4····IPPROTO_GGP·····IPPROTO_IP······IPPROTO_IGMP····IPPROTO_ICMP····SIO_RECVALL·RSDS×¦ì€°.hC•àÉRÛ'·á····ws2_32.pdb·········H‹Ä
```

Figure 1-IP Addresses Located in Unallocated Space

Further examination of the ICX clearly indicates that this system is also actively configured to communicate on a private network of 10.114.192.x with FTP settings to connect to 10.114.192.12 and 10.114.192.25. Also apparent is that at one time this system was configured to have the IP address 192.168.1.50. This IP address is also a private IP range. These IP configurations and artifacts definitively identify two things, 1) the device has been actively used for network communications and 2) that this device has communicated to public IP addresses not located in the United States. Further analysis and additional devices would be required to determine the timeframe of these public IP communications.

10) **<u>ESS DS400 Communications.</u>** A careful examination of the ESS DS400 devices and thumb drives was conducted. This examination proved that each DS400 had a Verizon cellular wireless communications card installed and that the card was active on powerup, which meant that there is the ability to connect to the public internet on these devices as well. Both of the DS400 devices were configured to transmit election results to IP address 10.48.51.1. This is a private network, which means that it would only be accessible by the remote DS400 systems through leveraging the public internet and establishing a link to a communications gateway using a public IP or via a virtual private network (VPN). It is important to understand that this

communication can only occur if the cellular modems have access to the public internet. I did not have the entire communications infrastructure for the private network and given this lack of device production associated with the DS200, I can not say which other devices may have connected to this private network nor the full extent of the communications of nor the remote accesses to the DS400 devices.

11) **Out of Date Security Updates and Virus Definitions.** An analysis of operating system, and antivirus settings on the servers and computers provided to me was conducted. It was immediately apparent that these systems were extremely vulnerable to unauthorized remote access and manipulation. For example, none of the operating systems had been patched nor the antivirus definition files updated for years. The Antrim EMS was last updated in 2016. The other systems were in a similar state. This lack of security updating has left these systems in an extremely vulnerable state to remote manipulation and hacking. Since 2016 more than ninety seven (97) critical updates have been issued for the Windows 10 operating system to prevent unauthorized access and hacking. The fact that these systems are in such a state of vulnerability, coupled with the obvious public and private internet access, calls the integrity of the voting systems into question. The Halderman report dated March 26, 2021 relating to this matter validates this finding. It also validates that the system is in a state such that an unauthorized user can easily bypass the passwords for the system and database to achieve unfettered access to the voting system in a matter of minutes. These manipulations and password bypass methodologies can be performed remotely if the unauthorized user gains access to the system through the private network or the public internet.

12) **Incomplete Compliance with the Subpoena for Digital Discovery.** Antrim County has apparently failed to produce all of the voting equipment for digital preservation and analysis. I

examined the purchase documents produced by Antrim County with respect to the purchase of the Dominion Voting system and note that the following system components listed on the purchase documents were not produced:

(a) ImageCast Listener Express Server

(b) ImageCast Express Firewall

(c) EMS Express Managed Switch

(d) ICP Wireless Modems (17)

(e) Image Cast Communications Manager Server

(f) ImageCast Listener Express RAS (remote access server) System

(g) ImageCast USB Modems (5)

Without these system components it will be impossible to determine the extent of public and private communications, the extent to which remote access to the voting system components is possible and to determine if or when unauthorized access occurred.

SIGNED UNDER THE PAINS AND PENALTIES OF PERJURY THIS 8th DAY OF April 2021.

Ben Cotton

Benjamin R. Cotton

EXHIBIT F

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**DECLARATION OF J. ALEX HALDERMAN IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION** **Civil Action No. 1:17-CV-2989-AT**

Pursuant to 28 U.S.C. § 1746, J. ALEX HALDERMAN declares under penalty of perjury that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

<u>Georgia's Current Election Technology</u>

2. Georgia recently deployed new voting equipment and software manufactured by Dominion Voting Systems, Inc. ("Dominion"). These components include ImageCast X Prime ("ICX") ballot marking devices ("BMDs"), ImageCast Precinct ("ICP") precinct-count scanners, ImageCast Central ("ICC") central-count scanners, and the Democracy Suite election management system ("EMS"). Georgia

Secretary of State Brad Raffensperger certified these components in August 2019,[1] and they were first used statewide during the June 20, 2020 election.[2]

3. Under this new system (the "BMD-based Election System"), Georgia generally requires all in-person voters to select candidates on Dominion ICX BMDs. These devices are computer tablets connected to off-the-shelf laser printers. They do not record votes but instead print paper records that are supposed to contain the voter's selections in both human-readable text and as a type of machine-readable barcode called a QR code. Voters insert these printouts into Dominion ICP optical scanners, which read the barcodes and count the votes encoded in them.[3]

4. Absentee voters do not use BMDs but instead complete hand-marked paper ballots ("HMPBs"), which are tabulated at central locations by Dominion ICC scanners. While Georgia's precinct-based ICP scanners have the capability to count hand-marked paper ballots,[4] the State only uses them to count BMD printouts.

[1] Georgia Dominion certification (Aug. 9, 2019), https://sos.ga.gov/admin/uploads/Dominion_Certification.pdf.

[2] Mark Niesse, "How Georgia's new voting machines work," *The Atlanta Journal-Constitution* (June 9, 2020), https://www.ajc.com/news/state--regional-govt--politics/how-georgia-new-electronic-voting-machines-work/RyIOJuHYQgktcCNGL9sEoK/.

[3] Decl. of Dr. Eric Coomer, Dckt. 658-2, at 10.

[4] *Id* at 9.

5. Pre- and post-election procedures in the BMD-based election system closely parallel those under the old DRE-based election system. Before every election, the Secretary of State's office prepares election programming files using Dominion EMS software, which is a collection of client and server programs that run on commercial-off-the-shelf (COTS) computers and servers. The Secretary of State transmits the election programming files to county officials, who use another instance of the Dominion EMS to prepare memory cards and USB sticks for every scanner and ballot marking device used in the county. These removable media contain the ballot design, including the names of the races and candidates, and rules for counting the ballots. Election workers install a memory card or USB stick into each BMD and ICP scanner prior to the start of voting.

6. After polls close, election workers remove the memory cards from every ICP scanner and return them to the county. At that point, the memory cards contain a digital image of each scan as well as the scanner's interpretation of the votes contained in the barcode. County workers use the Dominion EMS to retrieve data from the cards and prepare the final election results based on the barcode readings.

Attacks Against the BMD-based Election System

7. Attackers could alter election outcomes under Georgia's BMD-based election system in several ways:

(a) Attacks on the BMDs could cause them to print barcodes that differ from voters' selections. These changes would be undetectable to voters, who cannot read the encrypted barcodes. Since the barcodes are the only thing the scanners count, the impact would be a change to the election results. The only known safeguard that can reliably detect such an attack is to rigorously audit both the human-readable portion of the printouts and the barcodes, which Georgia does not currently do.

(b) Attacks on the BMDs could also change *both* the barcode and the human-readable text on some of the printouts. Research shows that few voters carefully review their BMD printouts, and, consequently, changes to enough printouts to change the winner of a close race would likely go undetected. No audit or recount could detect this fraud, since both the digital and paper records of the votes would reflect the same selections but not the ones the voters intended.

(c) Attacks on the scanners could also cause fraudulent election results by changing the digital records of the votes. The only known safeguard that can reliably detect such an attack is a sufficiently rigorous manual audit or recount of the paper records, which Georgia does not currently require.

8. One way that attackers could carry out attacks against the BMD-based election system is by infecting the election equipment with malicious software ("malware"). Malware could potentially be introduced in several ways, including: (a) with physical access to any of the many electronic components that compose the system, (b) through an attack on the hardware or software supply-chain, or (c) by spreading virally via the election management systems to polling place equipment during routine pre-election procedures.

9. Components of Georgia's election system that are not directly connected to the Internet might nonetheless be targeted by attackers. Nation-state attackers have developed a variety of techniques for infiltrating non-Internet-connected systems, including by spreading malware on removable media that workers use to copy files in and out.[5] Attackers could employ this method to infect the state or county EMS and spread from there to scanners and BMDs when workers program them for the next election. In this way, an attack could potentially spread from a single point of infection to scanners and BMDs across entire counties or the whole

[5] A well-known example of this ability, which is known as "jumping an air gap," is the Stuxnet computer virus, which was created to sabotage Iran's nuclear centrifuge program by attacking factory equipment that was not directly connected to the Internet. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired* (Nov. 3, 2014), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

state, in the same way that malware could have spread through the old DRE system, which was not effectively air-gapped or otherwise reasonably secured.

10. The BMD-based election system is at further heightened risk of attack because of the legacy of poor security in Georgia's old DRE-based election system and its associated computers and networks. If attackers infiltrated the DRE-based system, they likely did so by first infiltrating components such as the Secretary of State's computer network, the voter registration database software developed by PCC, Inc., or the non-"air gapped" computers and removable media used by state and county workers and outside contractors to transfer data into and out of the EMS. The record in this matter contains abundant evidence about vulnerabilities in all these components, some of which were unmitigated for years and may still be unmitigated. Responsibility for their security continues to rest with many of the same technicians and managers who oversaw the security of the old system and were unable or unwilling to implement effective security measures.

11. These components continue to be used with the new voting system, including to process data that is copied to polling-place equipment. If attackers breached any of them to attack the DRE-based system, those attackers may continue to have such access under the BMD-based system. Technologies that the State has highlighted as key defenses for these legacy components, such as anti-malware

scans, anti-virus scans, and endpoint protection, provide little defense against sophisticated attackers like hostile foreign governments.

12. Importantly, apart from the examinations Fortalice conducted that found significant vulnerabilities with the Secretary of State's information technology infrastructure including components of the election management network, there is no indication that Georgia has ever forensically or otherwise rigorously examined the current election system, including components from the prior DRE-based system that are used with the current BMD-based system. In an environment of advanced persistent threats to both election systems, coupled with the critical known vulnerabilities with those systems, the lack of any such examination raises serious concerns about the reliability of the current system and election outcomes.

Georgia's New Dominion Equipment has Critical Security Flaws

13. Dominion does not dispute that its products can be hacked by sufficiently capable adversaries.[6]

14. One reason why this is true is the complexity of the software, which far exceeds the complexity of the DRE-based system. The Dominion software used in

[6] Decl. of Dr. Eric Coomer, Director of Product Strategy and Security for Dominion ¶ 13, Dckt. No. 658-2 ("all computers can be hacked with enough time and access").

Georgia contains nearly 2.75 million lines of source code (equivalent to about 45,000 printed pages), excluding the Windows and Android operating systems and other off-the-shelf software packages.[7] The ICP scanner alone contains about 475,000 lines of source code, and its software is written in C/C++,[8] a programming language that is particularly susceptible to some of the most dangerous types of vulnerabilities.

15. Software of the size and complexity of the Dominion code inevitably has exploitable vulnerabilities. As a source-code review team working for the California Secretary of State concluded in a study of a voting system with only 10% as much code as Dominion's, "If the [system] were secure, it would be the first computing system of this complexity that is fully secure."[9] Nation-state attackers often discover and exploit novel vulnerabilities in complex software.[10]

[7] SLI Compliance, "Dominion Democracy Suite 5.10 Voting System Software Test Report for California Secretary of State" (Aug. 2019), https://votingsystems.cdn.sos.ca.gov/vendors/dominion/dvs510software-report.pdf.
[8] *Id.*
[9] Joseph A. Calandrino, Ariel J. Feldman, J. Alex Halderman, David Wagner, Harlan Yu, and William Zeller, "Source Code Review of the Diebold Voting System," in *California Secretary of State's Top-to-Bottom Review of Voting Systems* (July 20, 2007), https://votingsystems.cdn.sos.ca.gov/oversight/ttbr/diebold-source-public-jul29.pdf.
[10] Andrew Springall, *Nation-State Attackers and their Effects on Computer Security* (2019), Ph.D. dissertation, University of Michigan, https://deepblue.lib.umich.edu/handle/2027.42/143907.

16. In addition to its complexity, the Dominion software used in Georgia utilizes a wide range of outdated off-the-shelf software modules, including some that perform essential security functions, such as the operating system and modules that process files an attacker might have manipulated.[11] The oldest third-party software components appear not to have been updated in more than 15 years. This is unfortunately consistent with the DRE-based system, which relied on software so out of date that the manufacturer stopped providing updates and patches more than a decade ago.

17. Outdated software components are a security risk because they frequently contain known, publicly documented vulnerabilities that have been corrected in later versions. Old or outdated software used in Georgia's Dominion equipment includes a version of Microsoft SQL Server dating from 2016, Adobe Acrobat from around 2015, barcode scanner software from 2015, μClinux operating system software from 2007, COLILO bootloader software from 2004, and a version of the Apache Avalon component framework dating from 2002. Georgia's BMDs

[11] SLI Compliance, "Dominion Voting Systems Democracy Suite 5.5-A Certification Test Plan" 16-19 (Dec. 2018), https://www.eac.gov/sites/default/files/voting_system/files/DVS_Democracy_D-Suite_5.5-A_Modification_Test_Plan_v1.2.pdf.

use the Android 5.1.1 operating system,[12] which is almost six years old and has not received security updates since March 2018; as of August 2020, it contained 254 documented vulnerabilities.[13]

18. Georgia certified the Dominion system without performing its own security testing or source-code review. The certification was preceded by tests that were limited to checking functional compliance with Georgia requirements.[14] The test report states that the testing "was not intended to result in exhaustive tests of system hardware and software attributes."[15] The term "security" does not appear in the report.

19. Several months before Georgia certified the Dominion system, the State of Texas performed its own certification tests. The Texas certification was more comprehensive and included test reports from five examiners appointed by the Texas

[12] Certificate of Conformance, Dominion Voting Systems Democracy Suite 5.5-A (Jan. 30, 2019) at pp. 3-4, https://www.eac.gov/file.aspx?A=TQycVTA%2BOLpxoCbwCFjQJmJdRP1dq9sFO3oVUWJl5u4%3D.

[13] CVE Details, "Google Android 5.1.1 Security Vulnerabilities," https://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-19997/version_id-186573/Google-Android-5.1.1.html (last visited Aug. 19, 2020).

[14] Pro V&V, "Test Report: Dominion Voting Systems D-Suite 5.5-A Voting System Georgia State Certification Testing" (Aug. 7, 2019), https://sos.ga.gov/admin/uploads/Dominion_Test_Cert_Report.pdf.

[15] *Id*. at 3.

Secretary of State.[16] All of the examiners highlighted deficiencies with the Dominion system, including issues affecting its reliability, accessibility, and security. These problems led Texas to deny certification of the Dominion system in 2019.[17]

20. Several of the serious deficiencies noted by the Texas examiners affect system components used in Georgia, including the BMDs. One examiner noted that "the ICXs [BMDs] are built with a [commercial off-the-shelf] tablet and printer. The Android OS versions used on the tablets are several years old[;] therefore they do not have the latest security feature [*sic*.] as later Android releases."[18] A second examiner found that "[t]he doors covering data and power ports on the [BMD] tablets do not provide sufficient protection. […] a bad actor could add a USB device to the tablet while powered down that could remain undetected until after the election had ended."[19] A third examiner concluded that "[t]he ICX [BMD] also presented problems during the accessibility testing portion of the exam which demonstrate that it may not be suitable as an accessible voting system."[20]

[16] "Examiner Reports of Dominion Voting System Democracy Suite 5.5" (Jan. 16-17, 2019), https://www.sos.state.tx.us/elections/laws/jan2019_dominion.shtml.

[17] "Report of Review of Dominion Voting Systems Democracy Suite 5.5" (June 20, 2019), https://www.sos.state.tx.us/elections/forms/sysexam/dominion-democracy-suite-5.5.pdf

[18] Report of Texas examiner Tom Watson.

[19] Report of Texas examiner Brian Mechler.

[20] Report of Texas examiner Chuck Pinney.

21. Around the same time that Georgia certified the Dominion system, the State of California performed tests on a more recent version of the Dominion software, version 5.10, as part of its own certification process.[21]

22. In contrast to Georgia's tests, California's included some source code review and security testing. Like all security testing, the California tests were necessarily limited in scope and could not be expected to find all exploitable vulnerabilities. Nevertheless, they did uncover several serious flaws. These problems very likely apply to the version of the Dominion system used in Georgia given that it precedes the version tested in California.

23. The California testers found that attackers could modify the Dominion software installation files and believed that "it would be possible to inject more lethal payloads into the installers given the opportunity."[22] This implies that attackers could modify the Dominion installation files to infect election system components with malicious software.

[21] SLI Compliance, "Dominion Democracy Suite 5.10 Security and Telecommunications Test Report" (Aug. 2019), https://votingsystems.cdn.sos.ca.gov/vendors/dominion/dvs510security-report.pdf ("California Certification Security and Telecomm Test Report").

[22] *Id*. at 25.

24. Furthermore, the California testers found that the Dominion system's antivirus protection was insufficient or non-existent. "[O]n the EMS server, the AVAST Antivirus (AV) File Shield (the real time AV monitor) was only able to detect and clean one of the four [test] files. This potentially leaves the system open to zipped and double zipped viruses as well as infection strings in plain text."[23] Moreover, the ICX BMD and ICP scanner have no antivirus software at all.[24] As a result, malware that infected the Dominion components could evade antivirus detection.

25. One of the ways that attackers might affect election equipment is by physically accessing the devices. In the case of the Dominion BMD, the California source code reviewers found a vulnerability that can be exploited with physical access to the USB port that "would be open to a variety of actors including a voter, a poll worker, an election official insider, and a vendor insider."[25] This implies that no passwords or keys would be needed to exploit the problem, given physical access. California testers also found that "the ICX device does not provide monitoring of

[23] *Id*. at 19-20.

[24] *Id*. at 20.

[25] California Secretary of State's Office of Voting Systems Technology Assessment, "Dominion Voting Systems Democracy Suite 5.10 Staff Report" (Aug. 19, 2019) at 29, https://votingsystems.cdn.sos.ca.gov/vendors/dominion/dvs510staff-report.pdf.

physical security,"[26] and that, for all the polling place devices, including the ICX, "[s]ecurity seals, locks, and security screws can be circumvented."[27]

26. Other weaknesses found in the California tests include that "a number of passwords were able to be recovered that were stored in plain text,"[28] that the network switch used to connect EMS clients and servers was "determined to have twelve medium [severity] vulnerabilities and four low [severity] vulnerabilities,"[29] and that, if an authentication device used by poll workers and administrators was lost or stolen shortly before an election, revoking its access would require a logistically difficult process to reprogram the election files for the polling place devices throughout the jurisdiction.[30] These problems indicate that the Dominion system was designed without sufficient attention to security.

27. Although California ultimately permitted the Dominion system to be used, its certification requirements impose much more stringent security conditions

[26] California Certification Security and Telecomm Test Report at 11.
[27] *Id*. at 17.
[28] *Id*. at 15.
[29] *Id*. at 30.
[30] *Id*. at 15.

than those in Georgia, and no California jurisdiction uses Dominion BMDs for all voters as Georgia does.[31]

28. Dominion's response to Georgia's RFP lists among "key personnel" a "Chief Security Officer" (CSO) whose responsibilities for the voting system project were to be "Oversight of key security development and implementation."[32] Appointing a C-level executive to oversee a company's security posture is widely regarded as an industry best practice. However, at the time of the RFP, the CSO position was vacant, and to my knowledge Dominion has yet to fill the role.

BMDs and Ballot Barcodes Create Elevated Hacking Risks

29. Georgia's optical scanners use barcodes as the exclusive means of reading voters' choices. This increases the likelihood that attackers will be able to manipulate election results. The use of barcodes makes it possible for attackers to change how votes are recorded by hacking *either* the scanners or the BMDs. This

[31] California Secretary of State, "Conditional Approval of Dominion Voting Systems, Inc. Democracy Suite Version 5.10 Voting System" (Oct. 18, 2019), https://votingsystems.cdn.sos.ca.gov/vendors/dominion/ds510-cert.pdf.

[32] See "Original\0-4 Org Structure_Dominion and KNOWiNK - Redacted .pdf" at 3 *available at* https://sos.ga.gov/admin/uploads/Dominion.zip (last visited Aug. 19, 2020).

increases the "attack surface" of the election system: with two potentially vulnerable components to target instead of just one, attackers are more likely to succeed.

30. Georgia's Dominion ICX BMDs are computers, they run outdated and vulnerable software, and they must be programmed using the State's election management system before every election. Attackers could potentially infect Georgia's BMDs with malware in several ways, including by spreading it from the election management system (EMS).

31. An attacker who infected the BMDs with malware could change a fraction of the printouts so that the barcodes encoded fraudulent votes but the human-readable text showed the voters' true selections.

32. Voters would have no way to detect this attack. They cannot read the Dominion barcodes, which are encrypted, so it is impossible for them to verify whether the barcodes really match their selections. However, when the Dominion scanners tabulate BMD printouts, they ignore the printed text entirely and count only the votes encoded in the barcodes. This means that voters cannot verify the portion of their ballots that gets counted.

33. Such barcode attacks cannot be reliably detected using pre-election testing or parallel testing.[33] An attacker could decide which votes to modify based on a very large number of variables, including the time of day, the number of ballots cast, the voter's selections, and whether the voter used options such as a large font size or an audio ballot. It is impossible for any practical amount of testing to examine all sets of conditions under which attackers might choose to cheat.

34. In principle, a sufficiently rigorous audit that compared the human-readable portion of the printouts to the barcodes could detect such an attack. However, since attackers might choose to target any race in any election, every race and every election would need to be rigorously audited to rule out barcode-based fraud.

35. To my knowledge, Georgia has not announced plans to perform any kind of audit that would compare the barcodes and the printed text, nor what specific measures would be taken to render any potential audit sufficiently comprehensive and reliable.

36. Even if officials did detect that some ballots showed different choices in the barcode than in the text, there might be no way to determine the correct election

[33] *See* Philip B. Stark and Ran Xie, "Testing Cannot Tell Whether Ballot-Marking Devices Alter Election Outcomes" (2020), https://arxiv.org/pdf/1908.08144.pdf.

results. If the discrepancies resulted from an attack, this would cast doubt on *both* the barcodes and the ballot text. An attacker who was able to alter the barcode would be equally capable of altering the ballot text. Malware might be designed to sometimes alter only the barcode and sometimes only the text. This means that officials could not simply ignore the barcodes and count only the text if they suspected the BMDs had been compromised.

37. BMDs do not need to use barcodes. Several kinds of modern, EAC-certified BMDs deployed in other states do not use barcodes to encode votes. These include the Clear Ballot ClearAccess system[34] and the Hart Verity Touch Writer.[35] Instead of a barcode for vote tabulation, these systems print a ballot that looks like a hand-marked paper ballot but has scan targets filled in for the selected candidates.

38. In Dominion's response to the State's request for proposals, the company represented that an upcoming version of its BMD software would not need to print barcodes on ballots.[36] Instead, the BMDs would produce (and the scanners

[34] *See* Clear Ballot, "ClearAccess Accessible Voting," https://clearballot.com/products/clear-access.

[35] *See* Hart Intercivic, "Verity Touch Writer Ballot Marking Device," https://www.hartintercivic.com/wp-content/uploads/VerityTouchWriter.pdf.

[36] "Clarification Questions\MS 16-1 Supply Chain_Dominion and KNOWiNK Final.docx" *available at* https://sos.ga.gov/admin/uploads/Dominion.zip (last visited Aug. 19, 2020).

would count) an entirely human-readable ballot capable of verification by the voter. However, this option is described as an "upgrade" available only after "certification is complete at the EAC."

39. The Secretary of State's office and Dominion portray Georgia's BMDs as having this ability to print such a human-readable, "full-face" ballot. A video portraying such a capability is part of the "Important Voter Information" available to the public on the Secretary of State's elections security web page.[37] The video portrays a voter making her selections on a BMD displaying a mock ballot using Georgia state and local races and constitutional questions or referenda. At the end of the video, the voter selects "Print Ballot," and the attached printer produces a double-sided ballot with a darkened oval appearing next to the voter's selections.[38]

40. Dominion's in-precinct optical scanners already are capable of and certified to read such full-face paper ballots that do not encode votes using barcodes.

[37] https://www.dropbox.com/s/u0lc21u82ye2qpg/ICX%20BMD%20Cart.mp4, available through "Voting Cart" hyperlink at https://sos.ga.gov/securevoting (last visited Aug. 18, 2020).

[38] *Id.*

<u>BMDs Limit the Effectiveness of Voter Verification</u>

41. Even if Georgia were to implement rigorous post-election audits, BMDs make it possible for an attacker to compromise the auditability of the ballots and thereby undermine the primary goal of the paper trail. To do so, malware would cause the BMDs to sometimes print fraudulent selections in *both* the barcode and the human-readable text. This attack would be impossible to detect by auditing the printouts, because all records of the voter's intent would be wrong. Pre-election testing and parallel testing also cannot reliably detect such cheating.

42. Unlike the security of hand-marked paper ballots, the security of BMDs relies critically on voters themselves. The only practical way to discover a BMD attack that altered both the barcodes and the printed text would be if enough voters reviewed the printouts, noticed the errors, and alerted election officials. Yet several recent studies, including my own peer-reviewed research, have concluded that few

voters carefully review BMD printouts.[39,40,41] As a result, the BMD paper trail is not a reliable record of the votes expressed by the voters, and changes to enough printouts to change the winner of a close race would likely go undetected.

43. Even if some voters did notice that their selections were misprinted, these voters would have no way to prove that the BMDs were at fault. From an election official's perspective, the reporting voters might be mistaken or lying. Many voters would need to report that the BMDs misprinted their ballots before officials could be sure there was a systemic problem.

44. There are no protocols or policies in Georgia that I have found that address how many voter complaints, or other conditions, involving BMDs would be required within or across polling places to support a finding—or even a robust investigation—of a systemic problem. Moreover, it would be virtually impossible

[39] R. DeMillo, R. Kadel, and M. Marks, "What voters are asked to verify affects ballot verification: A quantitative analysis of voters' memories of their ballots" (2018). Available at https://ssrn.com/abstract=3292208.

[40] Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman, "Can Voters Detect Malicious Manipulation of Ballot Marking Devices?" in *Proceedings of the 41st IEEE Symposium on Security and Privacy* (Jan. 2020), https://jhalderm.com/pub/papers/bmd-verifiability-sp20.pdf.

[41] Philip Kortum, Michael D. Byrne, and Julie Whitmore, "Voter Verification of BMD Ballots Is a Two-Part Question: Can They? Mostly, They Can. Do They? Mostly, They Don't" (Mar. 2020), https://arxiv.org/ftp/arxiv/papers/2003/2003.04997.pdf.

for officials to recognize the subtle signs of a BMD misprinting attack during a chaotic election in which there were widespread equipment malfunctions and other problems, as occurred in Georgia during the June 9, 2020 primary.[42]

45. Even if officials did suspect that the BMDs had been attacked, there would be no straightforward way to respond or recover. One possible response would be to delay certifying the election results and conduct a forensic analysis to understand why ballots were misprinted and how many BMDs and votes were affected. Such an analysis might take months and would not be guaranteed to uncover a sophisticated attack. Yet if an attack were confirmed, there is little chance that its effects could be undone. The only recourse might be to rerun the election, which could be statewide involving millions of voters across Georgia.

46. Election officials are unlikely to take disruptive actions, like a protracted and expensive forensic investigation, unless a large enough fraction of BMD voters report problems. Suppose officials would launch an investigation if more than 1% of BMD voters reported a problem. If outcome-changing fraud occurred in an election with a 1% margin of victory, voters would need to verify their ballots so

[42] Richard Fausset, Reid J. Epstein, and Rick Rojas, "'I Refuse Not to Be Heard': Georgia in Uproar Over Voting Meltdown," *The New York Times* (June 9, 2020), https://www.nytimes.com/2020/06/09/us/politics/atlanta-voting-georgia-primary.html.

carefully that they would report 67% of the modified BMD printouts. This is *ten times* greater than the rate of error reporting measured in my peer-reviewed research.

<u>Reserving BMDs for Voters Who Request Them Would Strengthen Security</u>

47. When BMDs are used by all in-person voters, as in Georgia, there is a high risk that attackers could manipulate enough BMD votes to change the outcome of a close election without detection. Georgia is an outlier in adopting BMDs for all voters. As of December 2019, only 403 counties in the United States planned to do so, and almost 40% of them were in Georgia.[43] In contrast, the majority of election jurisdictions across the U.S. (representing nearly two-thirds of registered voters) provide BMDs exclusively for voters who request them (e.g., those with certain disabilities),[44] which is much safer.

48. Georgia can greatly strengthen the security of future elections through a straightforward procedural change. Rather than directing all in-person voters to use BMDs, the State could have in-person voters mark paper ballots by hand and reserve BMDs for voters who request to use them. This approach would require no additional equipment and would result in no loss in accessibility. Hand-marked

[43] Decl. of Warren Stewart, Dckt. 681-2.

[44] Verified Voting, *The Verifier*, https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2020 (last visited Aug. 18, 2020).

paper ballots are already used in Georgia for absentee voting, and so they are prepared and printed for every ballot style in every election. The state's new Dominion scanners are already capable of counting hand-marked ballots. BMDs would continue to be available for voters who need them. Yet the risk that election outcomes could be hacked would be far less than under Georgia's planned system.

49. Securing against misprinting attacks is much easier if only a small fraction of voters uses BMDs (without barcodes) and the rest use hand-marked paper ballots. This is because an attacker would be forced to cheat on a much larger fraction of BMD ballots in order to achieve the same level of fraud. In Maryland, which uses hand-marked paper ballots but makes BMDs available to voters who request them, about 2% of voters use BMDs. If only 2% of voters used BMDs in the scenario above (¶ 46), 1% of BMD voters would report a problem even if voters noticed only 3.8% of errors. Empirical studies suggest that voters really do achieve this modest rate of verification accuracy, even though it is unlikely they can achieve the far greater accuracy required to detect fraud when all voters use BMDs.

50. Using BMDs for all voters has no practical security advantages compared to reserving BMDs for voters who request them. On the contrary, it makes BMDs a much more attractive target for attackers and leads to greatly increased risks

for all voters—including the disabled—that their right to vote will be subverted by an attack on the BMDs. And regardless, there is no need for barcodes at all.

Georgia's Audits Provide Insufficient Protection

51. Rigorous post-election audits are necessary in order to reliably prevent attacks that compromise election results by manipulating ballot scanners. A rigorous audit would also serve to correct errors caused by scanners misreading ballots, to the extent that these errors resulted in an incorrect election outcome. However, as I have explained, post-election audits are not sufficient to detect attacks against BMDs, since such attacks could change both the printed and electronic records of the votes.

52. For an audit to reliably detect outcome-changing attacks, several requirements must be met. Among them are: (i) the paper ballots being audited must correctly reflect voters' selections; (ii) the audit needs to be conducted manually, by having people inspect the ballots without reliance on potentially compromised electronic systems or records; (iii) the auditors need to inspect sufficiently many ballots to ensure that the probability that outcome-changing fraud could go undetected is low. In general, the closer the election result in a particular race, the more ballots need to be audited in order to confidently rule out fraud. Audits that constrain the probability that the reported outcome differs from the outcome that

would be obtained by a full manual recount to no more than a pre-defined level (the "risk limit") are called risk-limiting audits ("RLAs").[45]

53. I understand that Georgia statute requires a state-wide post-election audit to be conducted no later than the November 2020 election.[46] However, that audit is not required to be risk-limiting. If it is not, and there are close races in which an attacker changes the outcome by hacking the election equipment, there is a high probability that the audit will fail to uncover the attack.

54. A proposed rule change recently noticed by the State Elections Board would require all counties to participate in a risk-limiting audit, but only following November general elections in even-numbered years.[47] Other elections, including state-wide primaries and runoffs, are not included in the requirement. Moreover, under the proposed rule, the RLA would target only one contest, which would be selected by the Secretary of State. Adversaries could choose to attack any race in

[45] *See* Mark Lindeman and Philip B. Stark, "A Gentle Introduction to Risk-limiting Audits," in *IEEE Security and Privacy* (2012), https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.
[46] *See* O.C.G.A. § 21-2-498(b).
[47] Georgia State Elections Board, "Notice of Intent to Post a Rule of the State Election Board, Title 183-1, *Rules of State Election Board*, Chapter 183-1-15, *Returns of Primaries and Elections* and Notice of Public Hearing" (Aug. 11, 2020), https://sos.ga.gov/admin/files/SEB%20Rule%20183-1-15-.02(2)%20and%20.04%20-%20To%20Post%20For%20Public%20Comment.pdf.

any election, and an attack would likely not be detected if it occurred in a contest that was not the target of the RLA or during an election for which no RLA was conducted. Even for the one contest every two years that would be audited, the proposed rule does not describe the auditing procedure in enough detail to evaluate its sufficiency. The specific process that election superintendents would follow to carry out the audit is yet to be defined.

55. No matter what auditing procedures Georgia applies, the state's widespread use of BMDs makes it possible for an attacker to undermine the integrity of the paper trail. Malware could cause the BMDs to print fraudulent selections, both in the barcode and the human-readable text. Such an attack would be impossible to detect by auditing the ballots, even with an RLA, because all records of the voter's intent would be wrong.

Hand-Marked Paper Ballots Are Much More Secure

56. Hand-marked paper ballots (HMPBs) are the most widely used voting technology in the United States. More than 65% of voters live in jurisdictions that use HMPBs as their primary in-person voting technology,[48] and all 50 states, including Georgia, use them for absentee voting. When used with modern precinct-

[48] Verified Voting, *The Verifier*.

count optical scanners and rigorous RLAs, HMPBs can provide much stronger security than BMD-printed ballots, especially those based on barcodes.

57. Virtually every class of attack that affects HMPBs also affects BMDs, but BMDs—especially those that use barcodes—additionally suffer from the serious possibility that malicious software will alter the voter’s choices without detection. In contrast, HMPBs can be well secured using existing election technology and procedural controls.

58. It is true that voters using hand-marked paper ballots sometimes make errors. However, modern ballot scanners, such as Georgia’s Dominion ICPs, can be programmed to detect the most common types of errors by voters, such as overvotes and undervotes. Where ballots are scanned in-precinct, and the scanners are programmed correctly, voters then have the opportunity to correct their ballots once the scanners report the errors. Scanners also sometimes misread voters’ marks, but such errors—to the extent that they affected an election outcome—would be detected and corrected during risk-limiting audits, which are necessary in any event in order to safeguard against outcome-changing attacks.

Georgia Elections Continue to be Threatened by Sophisticated Adversaries

59. Georgia’s election system continues to face a high risk of being targeted by sophisticated adversaries, including Russia and other hostile foreign

governments. These adversaries could attempt to hack the election system to achieve a variety of goals, including undermining the legitimacy of the democratic process and causing fraudulent election outcomes.

60. The Mueller Report recently outlined the scale and sophistication of Russia's efforts to interfere in the 2016 election, leaving no doubt that Russia and other adversaries will strike again.[49] The Special Counsel concluded principally that "[t]he Russian government interfered in the 2016 presidential election in sweeping and systematic fashion."[50] The report further explained that foreign actors "sought access to state and local computer networks by exploiting known software vulnerabilities on websites of state and local governmental entities."[51] The report also found that these foreign agents were successful in attacking at least one state and that their activities involved "more than two dozen states."[52] As noted prior to the Special Counsel's final report, Georgia was among the states that Russia targeted.[53]

[49] Special Counsel Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election (Volume I of II)*, United States Department of Justice (Mar. 2019), https://www.justice.gov/storage/report.pdf.
[50] *Id.* at 1.
[51] *Id.* at 50.
[52] *Id.*
[53] *See* Indictment ¶ 75, *United States v. Netyksho*, No. 1:18-cr-00215-ABJ, (D.D.C. July 13, 2018), ECF No. 1.

61. Russia has sophisticated cyber-offensive capabilities, and it has shown a willingness to use them to hack elections elsewhere even before 2016. For instance, according to published reports, during the 2014 presidential election in Ukraine, attackers linked to Russia sabotaged Ukraine's vote counting infrastructure, and Ukrainian officials succeeded only at the last minute in defusing vote-stealing malware that would have caused the wrong winner to be announced.[54]

62. Russia and other foreign governments continue to threaten Georgia's elections in 2020. As recently as this month, the U.S. Intelligence Community assessed that foreign threats to the 2020 election include "ongoing and potential activity" from Russia, China, and Iran, concluding that "[f]oreign efforts to influence or interfere with our elections are a direct threat to the fabric of our democracy."[55] These adversarial governments may "seek to compromise our election infrastructure

[54] Mark Clayton, "Ukraine election narrowly avoided 'wanton destruction' from hackers," *The Christian Science Monitor* (June 17, 2014), https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers.

[55] Office of the Director of National Intelligence, "Statement by NCSC Director William Evanina: Election Threat Update for the American Public" (Aug. 7, 2020), https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

for a range of possible purposes, such as interfering with the voting process, stealing sensitive data, or calling into question the validity of the election results."[56]

63. Georgia's BMD-based election system does not achieve the level of security necessary to withstand an attack by these sophisticated adversaries. Despite the addition of a paper trail, it suffers from severe security risks much like those of the DRE-based election system it replaced. Like paperless DREs, Georgia's BMDs are vulnerable to attacks that have the potential to change all records of a vote.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 19th day of August, 2020 in Rushland, Pennsylvania.

J. ALEX HALDERMAN

[56] *Id.*

EXHIBIT G

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**DECLARATION OF** **J. ALEX HALDERMAN** **Civil Action No. 1:17-CV-2989-AT**

Pursuant to 28 U.S.C. § 1746, J. ALEX HALDERMAN declares under penalty of perjury that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

2. I have reviewed the expert disclosures prepared by Dr. Juan Gilbert and Dr. Benjamin Adida for State Defendants. Neither Dr. Gilbert not Dr. Adida offers any rebuttal to the numerous, critical vulnerabilities in Georgia's BMDs that I described in my July 1, 2021 expert report. Dr. Adida did not respond to my report at all; State Defendants reissued prior declarations from him previously provided in this litigation. Neither of them disputes the presence of any of the serious

vulnerabilities I detail in my report or the steps I describe for exploiting those vulnerabilities to alter individual votes and election outcomes in Georgia. Nor does either of them claim to have examined any of the voting equipment used in Georgia to evaluate whether the vulnerabilities I identified—or others—have been exploited in any past election. Although each of them presumably could do this with the permission of State Defendants, who I understand engaged them as experts in this case, there is no indication either has undertaken any such inquiry or asked to do so. As a result, neither Dr. Gilbert nor Dr. Adida has anything to say about the reliability of the voting equipment used in Georgia elections. This is surprising, given that they have had at least the last year to examine Georgia's voting equipment.

3. State Defendants urgently need to engage with the findings in my report and address the vulnerabilities it describes before attackers exploit them. Nothing in Dr. Gilbert's or Dr. Adida's responses indicates that State Defendants understand the seriousness of these problems or have taken any measures to address them and their implications for the Plaintiffs' individual votes in future elections. Established practice in the security field would require State Defendants to promptly subject Georgia's voting system to rigorous testing in response to my report, to assess the extent and significance of each of the vulnerabilities I described, and to identify and *promptly implement* specific measures (where possible) to eliminate or mitigate each

of those vulnerabilities. Neither Dr. Gilbert nor Dr. Adida indicates any such efforts on their own part or on the part of State Defendants or anyone else. Again, Dr. Adida did not respond to my report.

4. In my report—a 25,000-word document that is the product of twelve weeks of intensive testing of the Dominion equipment provided by Fulton County—I find that Georgia's BMDs contains multiple severe security flaws. Attackers could exploit these flaws to install malicious software, either with temporary physical access (such as that of voters in the polling place) or remotely from election management systems. I explain in detail how such malware, once installed, could alter voters' votes while subverting all the procedural protections practiced by the State, including acceptance testing, hash validation, logic and accuracy testing, external firmware validation, and risk-limiting audits (RLAs). Finally, I describe working proof-of-concept malware that I am prepared to demonstrate in court.

5. My report concludes, *inter alia*, that Georgia's BMDs are not sufficiently secured against technical compromise to withstand vote-altering attacks by bad actors who are likely to target future elections in the state; that the BMDs' vulnerabilities compromise the auditability of Georgia's paper ballots; that the BMDs can be compromised to the same extent as or more easily than the DREs they replaced; and that using these vulnerable BMDs for all in-person voters, as Georgia

does, greatly magnifies the level of security risk compared to using hand-marked paper ballots and providing BMDs to voters who need or request them.

Reply to Declaration of Dr. Juan Gilbert

6. Rather than engage with the facts in my report, Dr. Gilbert responds largely with vague generalities. He gives no indication that he has ever used an ICX BMD, let alone tested its security. He begins by conceding that "any computer can be hacked," but he contends that "this general statement is largely irrelevant," because hand-marked paper ballot systems use computers too (to scan the ballots) (¶ 6). His position is inconsistent with accepted standards for election security and with the facts of the particular voting system used in Georgia.

7. My testing has shown that the BMDs used in Georgia suffer from specific, highly exploitable vulnerabilities that allow attackers to change votes despite the State's purported defenses. There is no evidence that Georgia's ballot scanners suffer from the same extraordinary degree of exploitability, nor does Dr. Gilbert contend they do. He ignores the relative ease with which Georgia's BMDs can be hacked, including by a voter in a voting booth in mere minutes. That extreme difference in security as compared to other voting technologies, particularly hand-marked paper ballots, is far from "irrelevant" as Dr. Gilbert implies.

8. Furthermore, even if the scanners were just as insecure as the BMDs, Georgia's practice of requiring essentially all in-person voters to use highly vulnerable BMDs would needlessly give attackers *double* the opportunity to change the personal votes of individual Georgia voters, since malware could strike either the BMDs or the scanners. Accepted standards in election security compel reducing points of attack for bad actors, not unnecessarily expanding them—a point Dr. Gilbert ignores.

9. Lastly, Dr. Gilbert also ignores that accepted election security protocols include an effective measure to protect against hacks of ballot scanners when the ballots are hand-marked rather than generated by BMDs—namely, reliable risk-limiting audits (RLAs), which would have a high probability of detecting any outcome-changing attack on the scanners. Not only do Georgia's BMDs defeat the efficacy of RLAs, but Dr. Gilbert continues to ignore the fact that Georgia requires an RLA of just one statewide contest every two years (and, to my knowledge, has not adopted specific, adequate procedures to ensure a reliable RLA for that one audit every other year).

10. Dr. Gilbert goes on to discuss issues related to voter verification of BMD ballots (which I respond to below). Yet he fails to address the potential for attackers to cheat by changing only the QR codes printed by Georgia's BMDs.

Voters cannot read the QR codes, but they are the only part of the ballots that the scanners count. My report details several routes by which malicious hardware or software can manipulate the QR codes and cause the recorded votes to differ from voters' selections. In principle, a rigorous risk-limiting audit would be likely to detect such an attack if the attacker changed enough votes to alter the outcome of the contest being audited, but again Georgia rules require such an audit in only a single statewide contest once every two years. As my report explains, this leaves the vast majority of elections and contests in Georgia vulnerable to QR code (and others) attacks, yet Dr. Gilbert says nothing about this threat.

11. Instead, Dr. Gilbert focuses exclusively on a different threat: attacks that change *both* the QR codes and the ballot text. In addition to the barcode-only attacks I just discussed, my report demonstrates that Georgia's BMDs can be manipulated so that both the barcodes and the printed text indicate the same fraudulent selections. No audit or recount can catch such fraud, because all records of the voter's intent would be wrong. The only reliable way to detect it would be if enough voters carefully reviewed their ballots, noticed that one or more selections differed from their intent, and reported the problems to election officials, *and* if Georgia officials then discerned from the pattern of voter reports that the BMDs were systematically misbehaving. Thus, Dr. Gilbert is mistaken when he contends that the distinction

between "voter-verifiable" and "voter-verified" paper ballots "only matters in principle" (¶ 7). All BMD ballots are potentially voter-verifiable, but unless enough BMD ballots are actually voter-*verified*, BMD-based attacks could alter election outcomes even in the rare instances where the State conducts a risk-limiting audit. And unless *every* BMD ballot is actually voter-*verified*, BMD-based attacks could alter individual voters' selections without detection..

12. A large body of recent scientific evidence has established that few voters are likely to catch errors caused by malicious BMDs. I have reviewed this evidence in previous declarations.[1] It comes from both field observations (which report how long real voters review their ballots during real elections) and laboratory tests (which report the fraction of errors that subjects detect when voting on hacked BMDs in simulated elections). These methodologies are complementary, and results to-date from all studies of both kinds point to a low rate of voter-verification.

13. Dr. Gilbert criticizes field observations because "[t]ime spent reviewing a ballot has little to do with whether it was actually verified" (¶ 9). This claim is inconsistent with accepted election security principles. Of course, they are not exactly the same question, but obviously the time spent reviewing a ballot can

[1] *Halderman decl.* (Dec. 16, 2019), Dkt. 682 at 23-33; *Halderman decl.* (Sept. 1, 2020) Dkt. 855-1 at 6-8, 55.

provide important insight into whether it was likely verified. For example, we can conclude that a voter who spends only a second or two reviewing a lengthy, complicated ballot is unlikely to have reliably verified each of their selections on the ballot. And of course, the same is true for a voter who spends no time at all reviewing their ballot. Review time is both practical to measure and clearly correlated with the error detection success, making it a valuable and relevant metric, as multiple studies confirm.

14. Dr. Gilbert seems to contend, without evidence, that a casual glance is sufficient to review Georgia-style ballots because selections are printed together with party affiliations (¶ 9). He cites no research (and I am unaware of any) that supports this conclusion, particularly when, as in Georgia, the party affiliations are printed in small type and in a different horizontal position for each contest. A real BMD ballot is reproduced on page 15 of my expert report. This is just one example of such a ballot; they can be longer and more confusing. Dr. Gilbert provides no basis for believing that voters would likely catch deliberate errors caused by compromised BMDs when voting such a ballot.

15. Dr. Gilbert references my award-winning peer-reviewed study about voter verification behavior, which found very poor rates of error detection and

reporting in a mock election using BMDs that my team hacked (¶ 10).[2] He contends that my study "ignores the reaction to such manipulation in an actual election, particularly one as heated in the public domain as the 2020 Election." (¶ 11). He does not explain how or why such circumstances would be expected to materially increase voter verification of their respective BMD ballots, nor does he cite any support for his claim to believe they would. And, just last week, the Atlanta Journal-Constitution obtained a study (under the Georgia Open Records Act) commissioned by the Secretary of State's Office in which researchers from the University of Georgia observed Georgia voters during the November 2020 election and reported how long they spent reviewing their BMD ballots.[3] Although it appears the Secretary of State had this study at the time of Dr. Gilbert's response to my report, he does not address or acknowledge it. The new study suggests that voters in the real world review their ballots *even less carefully* than voters in recent laboratory studies—despite the reminders election workers are supposed to give them to carefully review

[2] Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman, "Can Voters Detect Malicious Manipulation of Ballot Marking Devices?" In *41st IEEE Symposium on Security and Privacy* (May 2020). Available at https://ieeexplore.ieee.org/document/9152705.

[3] Mark Niesse, "Under half of Georgia voters checked their paper ballots, study shows," *Atlanta Journal-Constitution* (July 27, 2021). Available at https://www.ajc.com/politics/under-half-of-georgia-voters-checked-their-paper-ballots-study-shows/6HSVHHFOBRBDPODRZXLIBTUS64/.

their ballots at the polling sites, which Dr. Gilbert emphasizes as a remedy for poor voter verification of BMD ballots.[4]

16. The University of Georgia researchers report that 20% of voters they observed did not check their ballots at all.[5] Only about 49% examined their ballots for at least one second, and only 19% did so for more than five seconds. This is significantly worse performance than observed in my study, which found that when voters were verbally prompted to review their ballots before casting them, as should occur in Georgia, 63% of voters reviewed their ballots for only *two* seconds or more, compared to 19-49% in the new study.

17. This suggests that laboratory studies like mine tend to *overestimate* the rate at which real Georgia voters would detect errors on their BMD ballots. Since real Georgia voters were observed to review their ballots even less carefully than the

[4] Secretary Raffensperger appears to disagree with Dr. Gilbert about the value of measuring voter review time for assessing voter verification performance. He told the Atlanta Journal-Constitution that the new study "shows voters do indeed review their ballots for accuracy before casting them" and offers "proof the votes that were counted were for the candidates the voters intended." (*Id.*). I agree that the new study provides valuable insights about voter behavior, but, contrary to the Secretary's pronouncements, the results indicate that real Georgia voters are even less likely to detect errors caused by compromised BMDs than previous studies have suggested.

[5] Audrey A. Haynes and M.V. Hood III, "Georgia Voter Verification Study" (January 22, 2021). Available at https://s3.documentcloud.org/documents/21017815/gvvs-report-11.pdf.

participants in my study, it is reasonable to infer that real voters would catch an even smaller fraction of errors. The participants in my study who were similarly prompted to review their ballots caught 14% of errors. Therefore, real voters in Georgia are likely to catch substantially less than 14% of errors.

18. How often would voters have to detect errors on their BMD ballots to effectively safeguard against attacks? The answer depends on the margin of victory, since an outcome-changing attack would need to change fewer votes in a close contest. The model from my study shows that, given the margin of victory from the 2020 Presidential contest in Georgia, voters would need to have detected 46% of errors for there to be even one error report per 1000 voters, under a hypothetical scenario where the election outcome had been changed by hacked BMDs.[6] The University of Georgia observations show that barely 49% of voters looked at their ballots for even a second, let alone studied them carefully enough to reliably spot errors.

[6] To reiterate, the November presidential race was the only state-wide contest subjected to a risk-limiting audit. In other contests, attackers could change the outcome by tampering with only the ballot QR codes, and voters would have no practical way to detect this manipulation regardless of how diligently they reviewed their ballots.

19. Dr. Gilbert performs a similar calculation using the baseline error detection rate measured in my study. He finds that an outcome changing attack on Georgia's Presidential contest would have resulted in only 832 voters noticing that their BMD ballots showed the wrong selection. Dr. Gilbert suggests that there have not been such complaints from any voters, and says he finds it implausible that so many voters would have "simply not said anything or otherwise simply corrected their ballot and thought nothing of it then or since" (¶ 12).

20. This is an oddly constructed hypothetical, since Curling Plaintiffs do not claim here that the Presidential outcome was altered by hacking the BMDs. And Dr. Gilbert does not indicate any effort to determine the total number of spoiled ballots in Georgia's Presidential contest, which he presumably could have explored with State Defendants. Neither does he provide any basis to believe there were only 832 or fewer spoiled ballots. But suppose for the sake of argument that the Presidential election outcome in Georgia had been altered by hacking the BMDs, and there *were* complaints from the 832 voters that Dr. Gilbert has calculated. What then? It seems all but certain that these complaints would have been dismissed or drowned out in the cacophonous aftermath of the election or simply disregarded by election workers at the polling sites as voter errors. Yet the official count, the risk-limiting audit, and the recount would all have found the wrong winner, and there would be no

way to recover any altered vote or correct the election outcome short of rerunning the election. With a mere 832 complaints among 5 million participating voters (amidst a sea of other complaints, real and imagined), it is unlikely that poll workers or election officials, including State Defendants, would realize or even suspected there was a systemic problem with the BMDs, and it is completely implausible that they would take the drastic but necessary step of asking Georgians to vote again. Georgia's election system is susceptible to this extraordinary risk as long as it remains vulnerable to the attacks I described in my report (and potentially others).

21. To get to the point of making a decision to rerun an election, State Defendants (among others, perhaps) would first need to know how many voters discovered a problem when verifying their ballots. As Dr. Gilbert points out, the number of spoiled BMD ballots provides an upper bound on the number of voters who discovered and corrected an error (¶ 12). He does not say how many spoiled ballots there actually were in November 2020. If State Defendants knew the number was less than 832, they likely would have shared this fact with Dr. Gilbert, and he would have stated it in his report. It is reasonable to infer that either there were more than 832 spoiled ballots (and the attack is plausible) or State Defendants *do not know* how many BMD ballots were spoiled during the election, eight months later, despite

what Dr. Gilbert acknowledges those ballots would suggest about the reliability of the election.

22. That State Defendants may not know this information is consistent with gaps in other important election data that Georgia counties report to the Secretary of State. State Defendants recently produced electronic data (election projects) that I understand were required to be returned to them by counties after the November 2020 and January 2021 elections. In both elections, a large fraction of counties failed to return any data, returned the wrong data, or omitted data necessary for assessing the security and integrity of the result, such as election databases or ballot images. More than six months after these elections, the Secretary of State has not been able to assemble these electronic records and has not indicated any effort or willingness to do so. Yet the only way that State Defendants could use the number of spoiled ballots as a defense against BMD-based cheating would be if the poll workers accurately tracked it, counties accurately aggregated it, and the Secretary's Office received such data from across the state before the election result was determined. Even then, it is unlikely that the Secretary would be prepared to react by *rerunning the election* if the number of spoiled ballots exceeded the number predicted in an outcome-changing attack.

23. Given the ineffectiveness of such defenses and the critical security problems in Georgia's BMDs, I (like Dr. Appel) recommend that BMDs be reserved for voters who need or request them, as is the case in most states. Dr. Gilbert responds by claiming, without evidence, that "[d]isabled voters are even less likely to identify an error on their printed ballot" (¶ 14). I am unaware of any study that supports this sweeping indictment of voters with disabilities, which encompasses a vast array of disabilities that would not impact the ability of the voter to identify an error on their printed ballot in any way. He also contends that blind voters cannot detect errors on their ballot at all, but this is not true. Many blind voters use assistive technology to read printed text and likely could do so to verify their ballots. Moreover, only some voters who need BMDs are blind. For instance, those with motor impairments that prevent them from marking a ballot by hand would not necessarily have any greater difficulty verifying the printed text than any other voter. In any case, if BMDs are used primarily by voters with disabilities (as in most jurisdictions that use BMDs), they will represent a *much* smaller target,[7] and an

[7] Although Dr. Gilbert cites a figure that would imply that 10% of Georgians who voted in 2020 were disabled, data from Maryland, where BMDs are available upon request, suggests that only about 1.8% of voters would request to use BMDs if they were offered a hand-marked ballot first. (*Halderman decl.*, Aug. 19, 2020, Dkt. 785-2 at 49.) Dr. Gilbert's citation to the number of all Georgia voters with disabilities is highly misleading since, again, very few of those voters would be

outcome-changing attack on any given election will be detectable with a much lower rate of voter error detection than when all in-person voters use BMDs as they do in Georgia today. This in turn creates a strong disincentive for bad actors to attempt hacking an election (the risk likely is not worth the reward when the outcome is highly unlikely to be changed), which means individual votes would be less likely to be altered by hacking.

24. In his only direct response to my expert report, Dr. Gilbert states that he is not aware that I have "provided equipment marred by 'undetectable' hacks to any other independent researcher" (¶ 15).[8] This is a curious and ironic criticism coming from Dr. Gilbert, since he evidently chose not to evaluate my findings through an examination of the voting equipment himself, which he does not explain. Moreover, Dr. Gilbert misreads my report. It does not claim that malicious software infecting a BMD would be undiscoverable by any possible means. If an individual BMD is

unable to vote on a hand-marked paper ballot, consistent with the number reported in Maryland.

[8] Dr. Gilbert ignores that, as I understand it, State Defendants have objected to my report and the underlying work being shared with third parties (except Dominion), including other independent researchers, with whom I am eager to share my work for review. I am confident in my findings and believe they should be shared promptly with appropriate election security researchers and officials in an effort to mitigate the critical vulnerabilities in Georgia's voting equipment that I describe. I invite Dr. Gilbert to join me in seeking State Defendants' consent to do that.

known to contain malware, there will likely be some level of detailed forensic scrutiny that can detect where the malware is, perhaps requiring months of expert analysis per machine at extraordinary expense. It would be completely infeasible to perform this level of analysis on every machine before every election, much less between an election and the deadline for certification of its results. (And after manipulating ballots, malware could remove all traces of its presence from a machine, defeating any possible post-election examination of the device.) What my report shows is that vote-stealing malware of the type I have constructed would not be detected by any of the defenses that State Defendants purport to practice. I describe in detail how such malware would defeat QR code authentication, logic and accuracy testing, on-screen hash validation, and external APK validation (as was used by Pro V&V after the November election). Dr. Gilbert offers no rebuttal to these findings. He does not dispute them or even address them.

25. Moreover, there is already an example of an "undetectable" attack entered into testimony: exploitation of the Drupal vulnerability discovered by Logan Lamb in the Center for Election Systems server. As Lamb attested, the developers of the primary tool for detecting this vulnerability stated that "[n]either [the defensive tool] nor an expert can guarantee a website has *not* been compromised. They can only

confirm with certainty a website *has* been compromised."[9] Furthermore, the Drupal developers state that any server running the vulnerable software after the initial disclosure of the vulnerability should be assumed to have been compromised unless it was patched within *hours* of disclosure. According to the timeline presented in Lamb's declaration, he found the KSU server to be in a vulnerable state on August 28, 2016, nearly two years after the initial announcement of the critical vulnerability (October 15, 2014).[10] The KSU server image also contains evidence that a second vulnerability, the so-called Shellshock flaw, was exploited on December 2, 2014.[11] This vulnerability was publicly disclosed more than two months earlier and widely publicized in the media as a critical vulnerability, yet the KSU server remained unpatched.

26. An attacker who compromised the KSU server could therefore have maintained undetected access to the compromised server. Since the server remained in a vulnerable state undetected for almost two years, it is highly likely that it was successfully attacked at some point in time. An attacker who did so would have been able to move laterally to other systems within the CES network and to other

[9] *Lamb decl.*, Dkt. 258-1 at 19.

[10] See "Drupal Core - Highly Critical - Public Service announcement" (Oct. 29, 2014), available at https://www.drupal.org/PSA-2014-003.

[11] *Halderman decl.* (Sept. 1, 2020) Dkt. 855-1 at 23.

components of Georgia's voting system. As I have previously pointed out, many election system components that could have been compromised in this way are still in use in Georgia today, where they provide a means by which attackers could spread vote-stealing malware to the BMDs.

27. Rather than address the many threats to Georgia's voting system, Dr. Gilbert persists in drawing illogical comparisons between BMDs and hand-marked paper ballots. For instance, he questions why Plaintiffs have presented no research "regarding voters' proclivity to review [hand-marked paper ballots] to ensure their ballots are marked and will count as intended" (¶ 8). Much like Dr. Gilbert's earlier testimony that "[i]n essence, a BMD is nothing more than an ink pen,"[12] one does not need expertise in election security to find fault with this reasoning. Preventing voters from making accidental mistakes is a completely different problem from preventing their selections from being deliberately and systematically changed by an attacker who has compromised the BMDs. There is abundant evidence that voters do sometimes make errors whether filling out a ballot by hand or by machine. Bad ballot design exacerbates this problem with both voting modalities, but following ballot design best practices can greatly reduce it. Both

[12] *Gilbert decl.*, Dkt. No. 658-3 at 60.

BMDs and scanners that count hand-marked ballots can also be configured to reject overvotes and to warn voters about undervotes, the most common kinds of voter errors. Moreover, unlike older technologies for counting hand-marked ballots, the scanners used in Georgia (when properly configured) can detect improperly or incompletely marked bubbles and present them to human operators to adjudicate whether the marks should count as votes. Election officials can use all of these options to help protect voters from their own mistakes, but none of them offers protection against a BMD that deliberately changes the selections printed on a voter's ballot (or those encoded in the ballot barcode). The central problem with Georgia's highly vulnerable BMD system—that attackers can change all records of the voter's intent without being detected by election officials—has no parallel in a hand-marked paper ballot system.

28. Dr. Gilbert concludes as he started, with vague and sweeping generalities. "Simply put, BMD elections systems are no more insecure than [hand-marked] systems" (¶ 16). It is unclear whether he is claiming that *all* BMD systems are at least as secure as all hand-marked systems or merely that some specific BMD system (such as the one he recently developed himself to address some of the reliability problems that exist with Georgia's BMDs) is at least as secure as some hand-marked system, but this is of little consequence. The only BMD system that is

relevant here is the Dominion ICX as used in Georgia. As my expert report details, Georgia's BMD system suffers from numerous, severe vulnerabilities. These vulnerabilities would have little potential to change election outcomes if use of BMDs were limited to voters who need or request them, as Curling Plaintiffs desire, and they would be far less likely to affect the personal votes of individual Georgia voters.

Reply to Declarations of Dr. Benjamin Adida

29. The declarations by Dr. Adida that State Defendants have submitted predate my expert report, so Dr. Adida's opinions are not informed by the critical vulnerabilities in Georgia's BMD equipment that my analysis has revealed or by anything else in my lengthy, detailed report. Nor are they informed by any events that occurred in the year since he first provided these declarations, such as any aspect of the November 2020 election in Georgia or the Secretary of State's study indicating that few voters verified their respective ballots in that election.

30. Nevertheless, Dr. Adida's first declaration is correct that "Running a risk-limiting audit is one of the most important advances states can take in improving election integrity—without an RLA, we are effectively trusting computerized scanners to count our paper ballots" (Dkt. 834-2 at ¶ 5). This is true, but, as my expert report shows, without a risk-limiting audit Georgia is also trusting its critically

vulnerable BMDs to generate ballots with QR codes that correctly reflect voters' selections. Obviously compromised BMDs and compromised scanners could change individual votes and election outcomes. But again, nothing suggests that Georgia's scanners suffer from such easily exploitable critical vulnerabilities as the BMDs do.

31. Dr. Adida and I also agree that RLAs are important for discovering whether compromised BMDs have manipulated enough ballot QR codes to change the outcome of an election (¶ 12). Although RLAs are, as Dr. Adida says, "of the utmost importance" (¶ 6), Georgia does not require an RLA in the vast majority of elections and the vast majority of contests, leaving both election outcomes and individual voters' votes susceptible to manipulation via BMD malware. Additionally, it is insufficient for states to merely (in Dr. Adida's words) "take meaningful steps to implement RLAs"; rather, states have to *actually conduct* reliable RLAs, which Georgia does not intend to do for the vast majority of its elections (or perhaps any of its elections, depending on the reliability of the audit procedures it implements).

32. In his second declaration, Dr. Adida refers to a "dispute amongst academics regarding whether voters verify their ballots using ballot-marking devices" (Dkt. 912-1 at ¶ 11). This statement reflects a misunderstanding of the state of research today. I am not aware of any scientific research that supports the proposition that Georgia voters would likely detect more than a small fraction of

errors caused by BMD malware. In contrast, the past two years have seen a wave of laboratory studies and multiple field observation studies addressing this question, all of which strongly indicate the opposite, that few voters carefully review their ballots and so the vast majority of errors caused by BMD malware would likely to go undiscovered and uncorrected. Although there once was uncertainty about whether most voters carefully verify their BMD ballots, there is no longer any serious scientific dispute that they do not. It is the hallmark of good science (and of good public policy) that it evolves based on new evidence, such as the University of Georgia study commissioned by the Secretary of State that I discussed above—which Dr. Adida has not addressed.

33. Georgia's election system needs to evolve as well. Due to the critical vulnerabilities in Georgia's BMDs that are described in my expert report, Georgia voters face an extreme risk that BMD-based attacks could manipulate their individual votes and alter election outcomes. Even in the rare contests for which the State requires a risk-limiting audit, the scientific evidence about voter verification shows that attackers who compromise the BMDs could likely change individual votes and even the winner of a close race without detection. Georgia can eliminate or greatly mitigate these risks by adopting the same approach to voting that is practiced in most of the country: using hand-marked paper ballots and reserving

BMDs for voters who need or request them. Absent security improvements such as this, it is my opinion that Georgia's voting system does not satisfy accepted security standards. Neither Dr. Gilbert nor Dr. Adida offers a contrary opinion in their respective declarations, instead ignoring the critical issue of whether the *voting system used in Georgia*—which neither claims to have examined—reliably protects the right to vote for individual Georgia voters.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 2nd day of August, 2021 in Rushland, Pennsylvania.

J. ALEX HALDERMAN